Doors™ for use with Windows™

Access Control Software



Users Guide v5.9

(P/N 01914-100)

KERI SYSTEMS INCORPORATED

$49.00 USD

Document Number 01914-100, Revision 5.9 – April, 2006

SECTION NAME AND NUMBER	PART NUMBER	CURRENT REV.	REVISION DATE
Doors Users Guide	01914-100	5.9	April 2006
Section 1: Installation of Doors	01914-001	5.5	July 2005
Section 2: Set System Parameters and Verify Network Communication	01914-002	5.5	July 2005
Section 3: Database Programming	01914-003	5.4	May 2004
Section 4: Setup Users	01914-004	5.2	Sept. 2003
Section 5: Monitor and Update	01914-005	5.9	April 2006
Section 6: System Operation	01914-006	5.2	May 2004
Section 7: Reporting	01914-007	5.5	April 2006
Section 8: Multiple Sites	01914-008	5.3	Sept. 2003
Section 9: Photo Badge Management	01914-009	5.2	Sept. 2003
Section 10: EntraGuard	01914-010	5.4	April 2006
Section 11: User Data File Export/Import	01914-011	5.2	Sept. 2003
Section 12: Alarm Control	01914-012	5.5	March 2005
Section 13: Temp Users	01914-013	5.3	Sept. 2003
Section 14: Dual Verification	01914-014	5.5	Sept. 2003
Section 15: Video	01914-015	5.9	April 2006
Appendix, Glossary and Index	01914-100	5.9	April 2006

End of Section.

Users Guide

Table of Contents

End of Section.

Section 1

Installation of *Doors*

Document Number 01914-001, Revision 5.5 – July, 2005

Keri Systems, *PXL-250*, *PXL-500, PXL-510, SB-293*, *SB-593, Tiger Controller*, *EntraGuard*, *Doors, and Doors32* are trademarks of Keri Systems, Inc.

Acrobat® Reader © 1987-2001 Adobe Systems Incorporated. All rights reserved. Adobe and Acrobat are trademarks of Adobe Systems, Incorporated.

EPISuite is a trademark of G&A Imaging Ltd.

Windows is a trademark of Microsoft Corporation.

NetworX is a trademark of GE Interlogix.

This software is based, in part, on the work of the Independent JPEG Group. © 1991-1996.

The trademarks used in this Users Guide are the property of the trademark holders. The use of these trademarks in this Users Guide should not be regarded as infringing upon or affecting the validity of these trademarks.

1.0 *Doors*™ Users Guide

Doors is designed to make the access control system configuration and operation as simple as possible. This is done by breaking the configuration and operation processes into logical sections. Each section is responsible for a specific operation; whether it is entering information regarding how some aspect of the system is to be used or physically performing some operation.

This Users Guide is written for the novice user, learning how to navigate the *Doors* software menus and how to use the commands within the menus. The Users Guide presents the configuration and operation process in a recommended order of implementation. An operator can configure the system in almost any order, but the order described in the Users Guide provides the most sequential and complete path for the first time installer and for a new installation. Generally speaking, each section of the Users Guide builds upon what has been completed in the previous section.

2.0 Users Guide Conventions

To present this information, the Users Guide is written in simple step-by-step instructions.

There are certain conventions the Users Guide follows for presenting information and for indicating when an operator needs to perform an action on the computer.

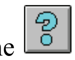
- **Items that require special attention or that can dramatically affect the access control network are prefaced by a caution sign and may be in bold face for extra emphasis.**
- Folder or directory names are identified in the text as "folder/subfolder."
- Information to be typed by an operator is identified in **Boldface**.
- If a button is clicked to perform an operation, the button icon is displayed or the button name is shown in **Boldface**.
- Locating an item under a pull-down menu is identified as Menu Option ⇒ Sub-Menu Option.
- Program names are identified in all UPPER CASE letters.
- Operation notes are shown in *italics*. These are things of which to be aware while using the *Doors* software.

Previous revisions of *Doors* software and controller firmware might not have all the features described in this Users Guide. This Users Guide is written to describe the capabilities of the current *Doors* software revision 4.20, PXL-250 controller firmware v6.3.54 (and later), PXL-500/ PXL-510 controller firmware v8.4.20 (and later), EntraGuard Gold controller firmware v7.3.10 (and later), and might not accurately reflect the capabilities of previous software/firmware revisions.

3.0 Windows Conventions

Doors is a fully compliant *Windows* program; providing complete operability in *Windows* and allowing its program window to be opened, closed, resized, and multi-tasked as any other *Windows* compliant program. Please refer to the help file within the *Windows* operating system for information on working in *Windows*.

4.0 Online Help

To assist the user the Users Guide is available as an online help file in the *Doors* software. To access the help file when in the *Doors* program, click on the Help/Contents pull-down menu or click on the  button on the *Doors* tool bar to open the help file (see Figure 1-13 on page 21 of this section).

5.0 Introduction to *Doors*

Doors for use with *Windows* is a software program that configures and manages an access control system using Keri Systems' PXL Tiger Controllers and/or EntraGuard Gold Telephone Entry Controllers.

Doors is a fully functional *Windows* program, making full use of all popular *Windows* features such as resizing and relocating windows, drag-and-drop functions, multiple windows open simultaneously, background operation, and real-time operation. *Doors* operates under *Windows 95*, *Windows 98*, *Windows 2000*, *Windows ME*, *Windows XP*, or *Windows NT v4.0*.

Doors provides the operator with a user-friendly interface for defining system parameters, managing cards/User IDs and transaction files, setting timing functions, and preparing reports. For operators who are familiar with spreadsheet programs (such as *Microsoft Excel*), many operations can be performed in spreadsheet format, using simple block, sorting, and copy functions. A wizard provides the operator a step-by-step walk-through procedure for enrolling cards/User IDs and creating Access Groups (a method for associating access doors with time periods of operation). An extensive online help file displays information with a click of the mouse.

A dedicated PC is not needed to run an access control network. The PC with the *Doors* program is only needed for entering and uploading information to the controllers, downloading information from the controllers, real-time network monitoring, and event data storage. *Doors* uses a proprietary communications protocol to automatically check all controllers on the network and then configures itself according to the connected hardware, greatly simplifying the system setup procedure. This proprietary communications protocol minimizes *Windows* General Protection Faults (GPFs) and system crashes.

Doors is capable of managing a single site via a direct connect serial line, a modem, or TCP/IP LAN-100, and is capable of managing up to 255 remote sites, each via modem or TCP/IP. Remote multiple site management features automatic dial-up of remote sites, global and site specific card/User ID enrollment, global and site specific event reporting, and configurable automatic downloads of events from controllers.

5.1 The *Doors* software can handle:

- Up to 32 system operators, each with password protection and configurable privileges.
- Up to 32 time zones (including dial time zones), each with 4 start/stop intervals.
- Up to 3 holiday schedules, each with up to 32 definable holiday dates.
- An unlimited number of Access Groups (subject to available hard disk space).
- Up to 6 sortable user definable text fields for individual user information.
- Up to 255 sites.
- Up to 128 controllers per site.
- Up to 128 doors (one per controller), or up to 256 doors (two per PXL controller) if using optional Satellite boards with every controller.
- A virtually unlimited number of cards/users for use with a PXL controller. Each controller can have its own set of users, but an individual controller can only handle the following number of cards.

	Standard RAM	Extended RAM	Temp Users Enabled	Temp Users Not Enabled
PXL-250	10,920	65,535	–	–
PXL-500/PXL-510	–	–	19,110	65,535

- Up to 750 User IDs to be assigned for use with an EntraGuard Telephone Entry controller.
- Each controller can store up to 3,640 events. These events can be transferred to the *Doors* software for storage on the host computer's hard disk and for event reporting.

6.0 Host Computer System Requirements

For proper operation of the access control system, the host computer running the *Doors* access control software must meet the following requirements.

- PC compatible computer using a Pentium-90 or faster microprocessor
- minimum of 16 MB of system RAM[1]
- SVGA color monitor with SVGA graphics card (800 x 600 minimum resolution for use with small fonts and 1024 x 768 minimum resolution for use with large fonts)
- CD-ROM, keyboard, and mouse or other pointing device
- 3.5 inch floppy disk drive or CD-ROM burner (optional for system backup)
- 50 MB of hard disk space
- COM port[2] with a 16550 UART to support an external modem or a direct RS-232 serial connection, or an internal 9600 baud (or faster) modem (EntraGuard units must use an external modem compatible with the internal EntraGuard modem)
- Ethernet card if using a LAN-100 for TCP/IP connection
- one of the following operating systems:

- *Windows 95*	- *Windows ME*
- *Windows 98*	- *Windows XP*[3]
- *Windows 2000*	- *Windows NT v4.0*

! ***Doors* is incompatible with Windows 3.11, Windows NT v3.51, and MS-DOS. *Doors* does not work with these operating systems.**

6.1 Photo Badge Management Requirements

For proper operation of *Doors* with a badging application, the following requirements must be met. These requirements supersede the standard *Doors* PC requirements.

- *Windows 95*, *Windows 98*, *Windows 2000*, *Windows ME, Windows XP Pro*[3] or *Windows NT 4.0* operating systems.
- The SVGA graphics card must be capable of displaying 65K colors to ensure photo images are properly displayed.
- Between 100 MB and 1 GB of hard disk space must be available, depending upon the number of users for which you will be providing photo badges. Refer to “Photo Badge Management” on page 3 in section 9 for further information on using the badging features of *Doors*.

! The TWAIN drivers that control communication between scanners or digital cameras and the badging software are not compatible with the Windows NT v4.0 operating system. Alternate methods for digital image transfer are necessary for these cameras.

---

1. The larger the number of users being enrolled, the larger the system RAM should be to efficiently handle the user database.
2. When connecting via an external modem or direct connect serial connection, all communication between controllers and the *Doors* software is done through the host computer's COM port. *Doors* cannot work if the host computer's COM port is not working correctly. Keri Systems cannot be held responsible for host computer COM port or hardware problems. With the *Doors* software package, Keri Systems provides a simple COM port test that can verify basic operation of the COM port. Please refer to the COMTEST Program section below for instructions on operating the program.
3. Although *Doors* is compatible with both *Windows XP* and *Windows XP Pro*, GuardDraw is certified to be compatible with *Windows XP Pro* only.

7.0 COMTEST Serial Port Test

The Keri Systems, Inc. COMTEST program is a simple program. It is designed to send a string of characters out the host computer's COM port output and see if they are echoed back to the host computer's COM port input.

It is not designed to determine if the COM port has more serious problems such as conflicts with other devices on the host computer. Troubleshooting by a computer technician is required to resolve these types of problems.

7.1 The Loop-Back Plug

To use the COM Test utility program, unplug the connection made from the access control system to the host computer's COM port. Plug in the loop-back plug. The loop-back plug routes the output signal from the serial port back to the input signal.

7.2 Starting COMTEST

1. Open the Windows Explorer program.
2. Locate the COMTEST.EXE program. For a default software installation the program can be found in the “\kerisys\Doors_vX.XX\utils” subdirectory (where X.XX is the revision of the *Doors* program).[1]
3. Double-click on the COMTEST.EXE program icon, or click on the COMTEST.EXE icon and then click on the File ⇒ Run pull-down menu option. COMTEST now begins.

7.3 Running COMTEST

1. When the program begins, the following screen appears.

```
KERI SYSTEMS INC. COMM TEST UTILITY

Plug in the Keri Loopback Test plug before starting the test.

Type C to set COM port
Type T to test COM port
Use icon in upper left to quit the program

PORT: COM2
STATUS: Untested
```

1. Earlier versions of *Doors* may be found in the “\kerisys\Doors32_vX.XX\utils” subdirectory.

2. Press the letter **C**. The following screen appears.

```
KERI SYSTEMS INC. COMM TEST UTILITY

Plug in the Keri Loopback Test plug before starting the test.

Type C to set COM port
Type T to test COM port
Use icon in upper left to quit the program

PORT: COM2
STATUS: Untested

Enter     1 = COM1, 2 = COM2, 3 = COM3, 4 = COM4
```

3. Press the number corresponding to the COM port the host computer is using for communication with the access control network (in this example, **2** is pressed). The following screen appears.

```
KERI SYSTEMS INC. COMM TEST UTILITY

Plug in the Keri Loopback Test plug before starting the test.

Type C to set COM port
Type T to test COM port
Use icon in upper left to quit the program

PORT: COM2
STATUS: Untested
```

4. Press the letter **T**. The following screen appears.

```
KERI SYSTEMS INC. COMM TEST UTILITY

Plug in the Keri Loopback Test plug before starting the test.

Type C to set COM port
Type T to test COM port
Use icon in upper left to quit the program

PORT: COM2
STATUS: Untested

Testing, please wait . . .
```

5. The COM port test takes just a few seconds. When complete, if the COM port has passed the test it is able to send and receive data. The following screen appears.

```
KERI SYSTEMS INC. COMM TEST UTILITY

Plug in the Keri Loopback Test plug before starting the test.

Type C to set COM port
Type T to test COM port
Use icon in upper left to quit the program

PORT: COM2
STATUS: Passed
```

6. If the COM port has failed the test, the following screen appears (the error message will vary depending upon what type of error was detected).

```
KERI SYSTEMS INC. COMM TEST UTILITY

Plug in the Keri Loopback Test plug before starting the test.

Type C to set COM port
Type T to test COM port
Use icon in upper left to quit the program

PORT: COM2
STATUS: Failed

An error has occurred <type of error>
Press any key to continue
```

7. To rerun COMTEST, press any key to return to the beginning of the program.
8. To exit the program, either click on the ☒ box in the upper-right corner of the COMTEST window, or click on the Windows icon in the upper-left corner of the COMTEST window and a pull-down menu appears. In the menu, click on **Close**.
9. Remove the loop-back plug from the serial port and reinstall the communication cable.

7.3.1 If the Host Computer Fails COMTEST

If the host computer fails COMTEST, there is a basic problem in transferring data through the COM port. Troubleshooting by a computer technician is required to resolve the problem.

7.3.2 If the Host Computer Passes COMTEST, but there are Still Problems

The COM Test will pass if it tests a port with an installed modem. To verify the correct port is being tested, unplug the loop-back plug and rerun the test. If the correct port is being tested, the port should fail (since the loop-back plug is not installed). If the COM Test passes, either an incorrect port is being selected, or there is an internal problem that the COM Test does not recognize.

Some COM port problems are beyond the scope of this COM test program. These types of problems tend to involve several devices within the computer that are trying to use the same resources within the computer, each device affecting the others. Troubleshooting by a computer technician is required to resolve the problem.

7.4 Set the Host Computer Date and Time

To ensure that the date and time assigned to events on the access control system are correct, the date and time kept by the host computer should be checked for accuracy. Part of the controller configuration process is to set the time and date of the controllers to match that of the host computer.

NOTE: If the Doors program is running, please close the program before setting the host computer's date and time. Closing the program ensures that when the Doors program is started, all timing functions are based on a correctly set host computer clock.

1. Double-click on the 2:41 PM field on the Windows Task Bar. A clock/calendar window appears (see Figure 1-1).

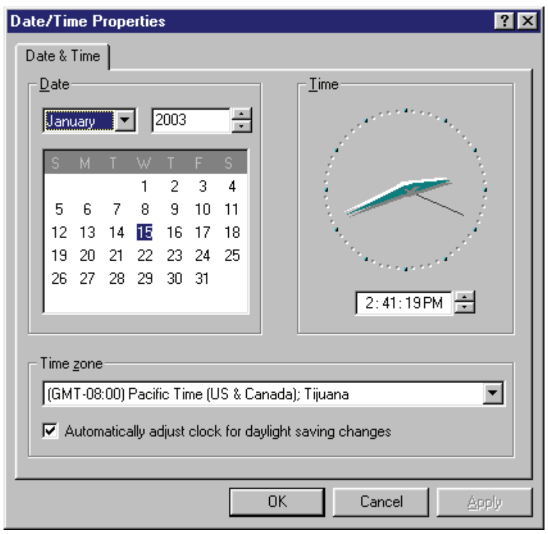


Figure 1-1: Host Computer Clock/Calendar Window

2. To set the time, double-click on the hours field of the digital clock display. Click on to advance the clock to the correct hour. Repeat this process for the minutes, seconds, and A.M./P.M. setting.
3. In the Time zone field, click on and a list of time zones appears. Scan through the list and click on the time zone corresponding to where the computer is located. If you live in an area that uses Daylight Savings Time, click in the box beside the "Automatically adjust clock for daylight savings changes" check box. A check mark in the box enables the automatic adjustment feature.
4. To set the month, click on the in the month field and a list of months appears. Scan through the list and click on the month.
5. To set the year, click on to advance to the correct year.
6. To set the day, click on the day in the calendar.
7. Click the OK button and the time and date are set in the host computer.

NOTE: International date and time formats are supported by the Doors program. The program displays and reports dates and times in the format selected when setting the host computer's date and time.

8.0 Software Installation

This section covers the following types of installations.

- a new installation of *Doors* software
- upgrading an existing *Doors* software installation to a new revision
- performing certain installation maintenance tasks

NOTE: If you are installing Doors with Badging, beginning with v3.74, the Doors software prepares your installation/upgrade depending on what your system currently has in use. The installation wizard will guide you through the process with system specific directions.

8.1 Installing Doors Products

An InstallShield wizard handles the software installation/upgrade process. Installing software is basically a question and answer process. To accommodate the installation process and install *Doors* software the host computer must meet the system requirements detailed in "Host Computer System Requirements" on page 6 of this section.

The installation program tests for these host computer minimum standards before starting the software installation process. If the host computer does not meet these minimum standards the installation program will not run; it exits to the Windows operating system.

1. Load the installation CD into the CD-ROM of the host computer. The AutoRun Menu appears.
2. Click on the Keri product that needs to be installed or updated.
3. Follow the on-screen step-by-step instructions.

8.1.1 Adding Dealer Help Information to *Doors*

It is possible to add specific dealer information that will appear in the *Doors* About window (see Figure 1-4 on page 12 of this section.

1. Open the text editor program (eg. Notepad). Enter the information to be displayed on the About screen in the Doors program (see Figure 1-2).

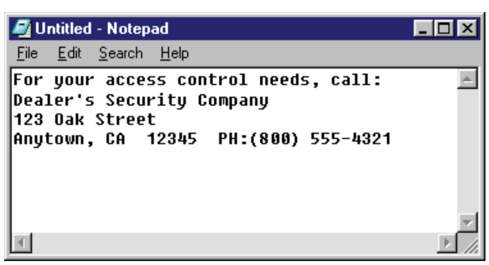


Figure 1-2: Dealer Information in Notepad

2. Click on the File ⇒ Save As pull-down menu option. The Save As window appears.
3. Locate the folder where the Doors.EXE program file is located (typically found in the "\Kerisys\Doors_vX.XX" folder). In the File Name field, type "dealer" and make sure the Save As Type field has "Text Documents" selected (see Figure 1-3).

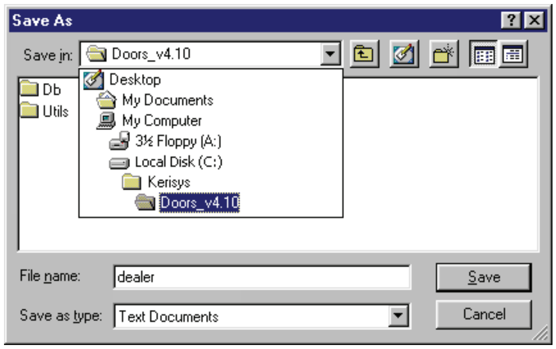
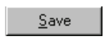


Figure 1-3: Save As Window

4. Click on the  button.

Each time the Help ⇒ About pull-down menu option is selected, the *Doors* About screen will include the dealer information (see Figure 1-4 on page 12 of this section).



Figure 1-4: *Doors* About Window with Dealer Information

8.1.2 Adding Dealer Splash Page to *Doors* Startup

A splash window may be added to the *Doors* Startup with the dealer logo and information. The splash window must be a Windows bitmap. It may be a scan of a business card, company logo, or the output of just about any paint program, including the one that ships with Windows. Keri suggests you keep the graphic to no larger than 400 x 400 pixels. To be completely universal, it should be 256 colors with an optimized palette.

NOTE: If a true color bitmap is displayed on a 256 color monitor, the graphic will probably be very ugly and possibly unreadable.

To add a splash window to the *Doors* Startup:

1. Once the graphic has been chosen, save it to the folder where the Doors.EXE program file is located (typically found in the "\Kerisys\Doors_vX.XX" folder) with the name of "dealerfile.bmp".
2. Next, locate the  shortcut icon on the host computer's desktop.

3. Right click on the shortcut and select “Properties.” The Properties window will appear (see Figure 1-5 on page 13 of this section).

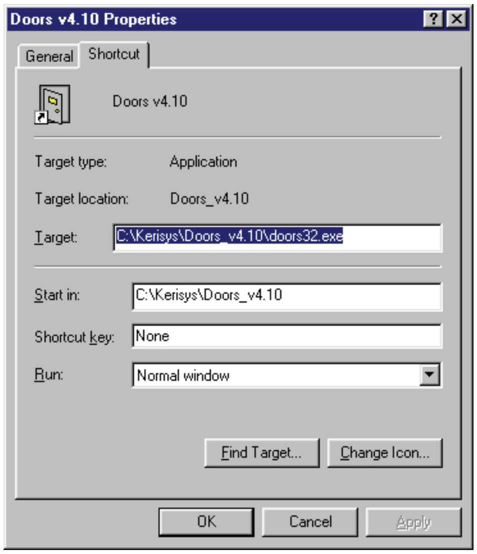


Figure 1-5: Doors Shortcut Properties Window

4. Locate the Target field. Following the path “C:\Kerisys\Doors_v4.10\doors32.exe” add the phrase “-bdealerfile.bmp”.
5. The default display time is set for 15 seconds. To change the display time, add the phrase “-txx” following “C:\Kerisys\Doors_v4.10\doors32.exe -bdealerfile.bmp” (xx must be a number between 01 and 30 which represents the length of time, in seconds, that the splash window will display). See Figure 1-6.

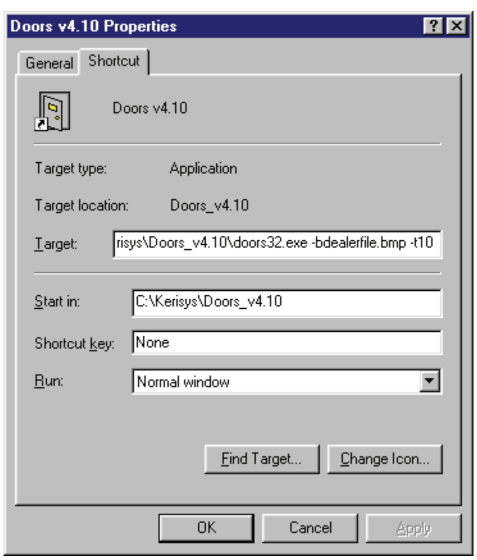


Figure 1-6: Doors Shortcut Properties Window with Splash Path and Display Time

6. Each time the *Doors* program is started, the set splash window will precede the *Doors* splash.

9.0 Installation Maintenance

The following section provides information on verifying host computer system resources for optimum program operation, for running a previous *Doors* installation, and for deleting a previous *Doors* installation.

9.1 Verify Host Computer System Resources

Sporadic problems in operating the *Doors* program can be due to an inadequate amount of the host computer's resources being available for use by *Doors*. The greater the number of programs open concurrently, the less the amount of system resources available for any one program. *Doors* needs approximately 65% of the computer system's resources free for proper operation. Perform the following steps to verify system resources.

1. Click on the Start button on the Task Bar. A menu of selections appears.
2. Click on Settings ⇒ Control Panel.
3. When the Control Panel window appears, double-click on the **System** icon.
4. When the System Properties window appears, click on the **Performance** tab.
5. A list of system performance status values will appear; one of which is the system resources value.
6. The system resources value should be above 65% to ensure proper operation of the *Doors* program. If it is not, close other unneeded programs to release the system resources they are using.
7. When you have finished viewing the system performance values, click on the **OK** button or click on the ☒ box in the upper-right corner of the window.
8. If closing programs does not release enough system resources, close all programs, re-boot the host computer, and then start the *Doors* program. This releases all system resources for reallocation.

9.2 Operating a Previous *Doors* Installation

At times following an upgrade installation, it might become necessary to revert to the previous installation of *Doors* software. As the *Doors* installation wizard creates a unique directory for each revision it installs of the *Doors* software, the previous revision is left intact. Operating the previous *Doors* software revision is simply a matter of locating and running the correct *Doors* executable program.

1. Open the Windows EXPLORER program.
2. Locate and click on the folder for the previous software revision (this is typically found in the "c:\kerisys\Doors_vX.XX[1]" directory).[2]
3. If the Doors v4.10 shortcut is visible, click on and drag the icon from the EXPLORER window to the Windows desktop.
4. If the shortcut is not visible, right-click on the doors.exe application file. A list of menu options appears. Scroll through this list and click on the **Create Shortcut** menu option. A shortcut to the previous installation of *Doors* is created and placed in the software folder.
5. Click on and drag the Shortcut to doors file from the EXPLORER window to the Windows desktop.
6. To run the previous installation of *Doors*, double-click on the *Doors* shortcut icon on the Windows desktop.

! *NOTE: If you are downgrading from Doors 32-bit to Doors 16-bit software there are specific firmware requirements for the master controller. Please contact your Keri Systems dealer for firmware revision information.*

---

1. X.XX refers to the revision of the *Doors* program.
2. Earlier versions of *Doors* may be found in the "c:\kerisys\Doors32_vX.XX" directory.

9.3 Deleting a Previous Installation of *Doors*

If the new *Doors* installation has been operating correctly for an extended period of time and if disc storage space is at a premium, the previous installation can be deleted.

Be sure the new installation is working to your satisfaction before deleting the previous installation. Once deleted, the previous installation cannot be recovered and all database information associated with this installation is lost.

1. Click on the Start button on the Task Bar. A menu of selections appears.
2. Click on Settings ⇒ Control Panel.
3. When the Control Panel window appears, double-click on the **Add/Remove Programs** icon.
4. An Add/Remove Programs Properties window appears. In the bottom half of this window is a list of installed programs. Scroll through this list of programs and locate and click on the *Doors* listing you wish to remove from the host computer (see Figure 1-7).

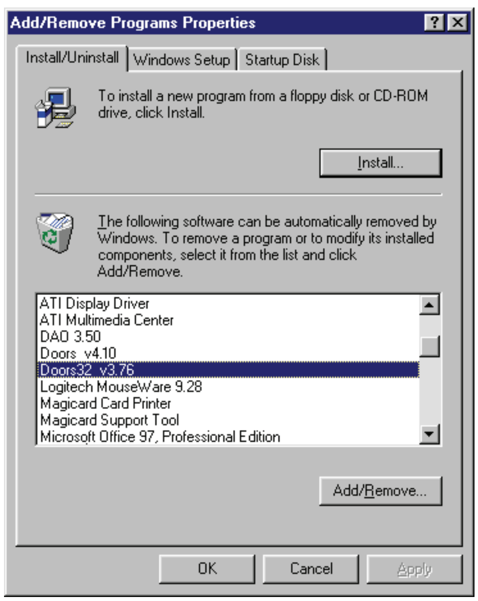


Figure 1-7: Add/Remove Programs Properties Window

5. Click on the Add/Remove... button.
6. A *Doors* Removal Confirmation window appears.

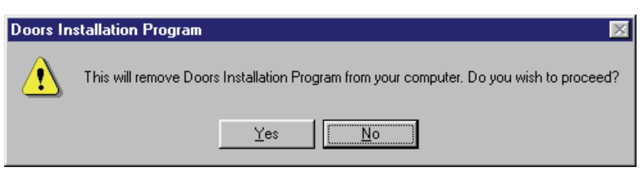


Figure 1-8: *Doors* Removal Confirmation Window

7. Click on the Yes button.
8. The uninstall program begins and a Remove Programs window appears (see Figure 1-9 on page 16 of this section).

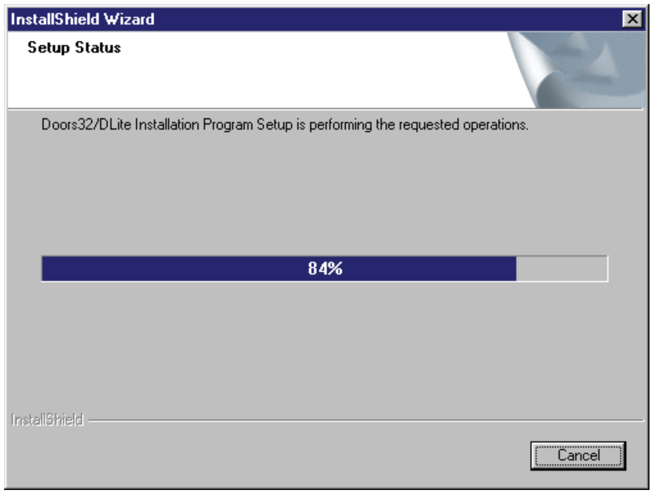


Figure 1-9: Remove Programs Status Window

9. Once the program removal process is complete, the *Doors* Removal Complete window appears (see Figure 1-10).

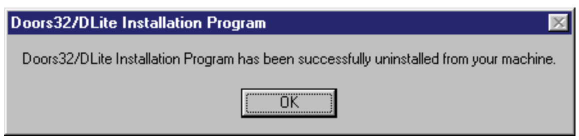
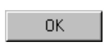


Figure 1-10: *Doors* Removal Complete

10. click on the 

button. The previous installation is deleted and disc storage space is recovered.

10.0 Product Documentation

Doors installation software is released in a CD-ROM format. The CD-ROM format includes copies of product documentation in Adobe Acrobat PDF format, and it includes a copy of the Adobe Acrobat Reader installation program. The Adobe Acrobat PDF – portable document format – allows an end user to easily view and print copies of documents encoded in the PDF format.

Two document folders are on the CD-ROM: Marketing_Documents and Technical_Documents. Each folder has sub folders that break out product documentation according to product type.

NOTE: The documents on the CD-ROM are the current revisions at the time of CD-ROM release. However, these documents are subject to change at any time. If necessary, please contact Tech Support at Keri Systems to verify the current revision of any document.

10.1 Installing the Acrobat Reader Program

If the Acrobat Reader is not already installed on your host computer, follow these instructions to run the Reader installation program.

1. Insert the *Doors* installation CD-ROM in to the host computer's CD-ROM drive.
2. From the AutoRun Menu (see Figure 1-2 on page 11 of this section), click on the **Install the Acrobat Reader** link. The installation program begins.
3. The Acrobat Setup Wizard will take you through the installation process.
4. When the installation process is complete, an Acrobat Reader shortcut will be placed on the host computer's desktop.

10.2 Accessing Documentation

Once the Acrobat Reader program has been installed on the host computer, there are two ways to access product documentation on the *Doors* CD-ROM – using the Acrobat Reader program directly or using Windows Explorer.

10.2.1 Using the AutoRun Menu and Windows Explorer

1. Insert the *Doors* installation CD-ROM in to the host computer’s CD-ROM drive.
2. From the AutoRun Menu (see Figure 1-2 on page 11 of this section), click on the desired link (Explore the CD-ROM, Locate Technical Documentation, or Locate Marketing Documentation). If you chose the Technical or Marketing Documentation links, a sub-menu appears. Once you have made another selection (or if you select Explore the CD-ROM), the Windows Explorer is automatically opened to the desired location with a list of the available PDF documents.
3. Scan through the list of PDF files and double-click on the desired file. The Reader program opens with the selected file as its contents.

10.2.2 Using the Acrobat Reader Program

1. Double-click on the Acrobat Reader shortcut icon. The Reader program opens.
2. Click on the File ⇒ Open pull-down menu option. A standard Windows open file window appears.
3. Use the navigation tools to display the contents of the desired folder on the *Doors* CD-ROM (in either Marketing_Documents or Technical_Documents). A list of PDF documents appears.
4. Scan through the list of PDF files and either double-click on the desired file, or click on the file and then click on the 

button. The file appears in the Reader window.

11.0 Starting *Doors*

The first step to start the *Doors* program is to log onto the system. In normal operation, the logon process identifies to the software which operator is entering the program. With this identification, the program is able to limit the operator's actions to those that the operator has been approved to perform.

11.1 Starting the Program

There are several ways to start the *Doors* program. The easiest, most common methods are described below.

11.1.1 From the *Windows* Task Bar

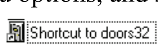
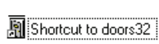
1. Click the  button. A pop-up menu of commands appears.
2. Click the **Run...** menu option. A pop-up dialog box appears.
3. Click the  button. A list of program folders appears.
4. Locate the Doors.EXE program file (typically found in the "\Kerisys\Doors_vX.XX" folder).
5. Click on the  program file. Click on the  button and the file path appears in the "Open" field.
6. Click the  button.
7. The program now begins.

11.1.2 Using WINDOWS EXPLORER

1. Run the WINDOWS EXPLORER program.
2. Locate the  program file (it is typically found under the "\Kerisys\Doors_vX.XX" folder).
3. Either double click on the  program file or click on the file to highlight it and then click on the File ⇒ Open pull-down menu.
4. The program now begins.

11.1.3 Using a Windows Desktop Shortcut

A desktop shortcut should have been automatically created during the installation process. However, if no shortcut can be found, the following instructions will guide you through the process of creating a shortcut for the desktop.

1. Run the WINDOWS EXPLORER program.
2. Locate the  program file (it is typically found under the "\Kerisys\Doors_vX.XX" folder).
3. Click on the  program file. It should now be highlighted.
4. Either click on the File ⇒ Create Shortcut menu option or right click the  program file, scroll down the list of menu options, and select the Create Shortcut option.
5. A new file is created titled  .
6. Click and hold the  program file and drag it to the computer screen desktop.
7. Close the WINDOWS EXPLORER program.
8. This icon now appears on the desk top every time the *Windows* program is started. Simply double click on the icon to start the *Doors* program.

11.2 System Logon

Once the program begins, it will prompt for an operator logon (see Figure 1-11). This is an identifying name and password for the operator entering the program. The first time the program is entered, the default logon information must be used. Until changed, the default password provides access to everything in the *Doors* program. Later in the *Doors* configuration process, each authorized operator is assigned identifying names and passwords (see “Setup Operators” on page 45 in section 2).

11.2.1 To Log On the *Doors* Program

1. Click in the “Name” field, type the name of the operator logging on and press **ENTER** (the default for this field is **Keri**).
2. Click in the “Password” field, type the password assigned to the operator listed in the name field (the default for this field is **Keri**). Asterisks appear in the password field instead of letters so that someone looking over your shoulder while you log on the program cannot learn your password.

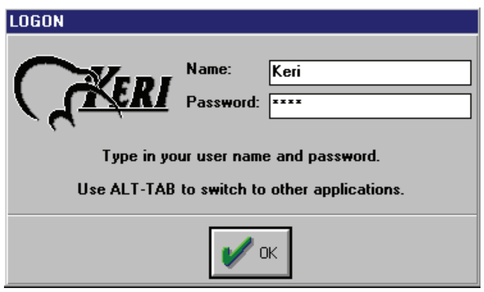


Figure 1-11: Logon Window

3. Click on the  button.

The program will now verify the operator name and password. If both are correct, the Logon window disappears allowing access to the *Doors* program. If either are incorrect, the name and password fields are cleared and the Logon window remains.

NOTE: The operator name and password are both case sensitive. That is, the program differentiates between UPPER CASE and lower case in both the operator name and password. Please keep this in mind when creating operator names and passwords, and when entering your operator name and password to log on the Doors program.

11.2.2 To Log Off the *Doors* Program

Whenever one operator replaces another operator, for instance during a shift change, the original operator should log off the system and allow the new operator to log on. This provides for correct tracking of which operator initiated events during the shift.

1. Click on the File ⇒ Log Off pull-down menu option. The original operator is logged off the system and the Logon window appears (see Figure 1-11).
2. Before any other operation can be performed, the new operator must log on the system as described in “To Log On the Doors Program”.

11.3 Initial Network Update

The first time the program starts, a "Network Update" window appears (see Figure 1-12). The Network Update window indicates that first-time communication between the *Doors* program and the access control network has not yet been made.

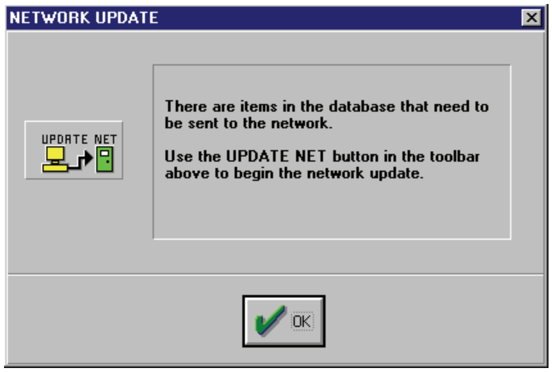


Figure 1-12: Network Update Window

In the future, whenever starting the program, this window appears if a change has been made to any *Doors* database that has not yet been sent out to the access control network. This window serves as a reminder that changes in the database are not physically implemented in the access control network until they have been uploaded to the access control network.

1. Click on the  button to enter the *Doors* desktop.

NOTE: This is just a reminder window. When you click on "OK" you have not updated the network. To update the network see "Update the Network" on page 35 in section 5.

12.0 Introducing the *Doors* Desktop

Every task in *Doors* is begun from the desktop. Navigating the desktop is simply a matter of using the mouse to point and click on items, and entering appropriate information when needed.

12.1 The Desktop

There are eight fields on the *Doors* desktop (see Figure 1-13).

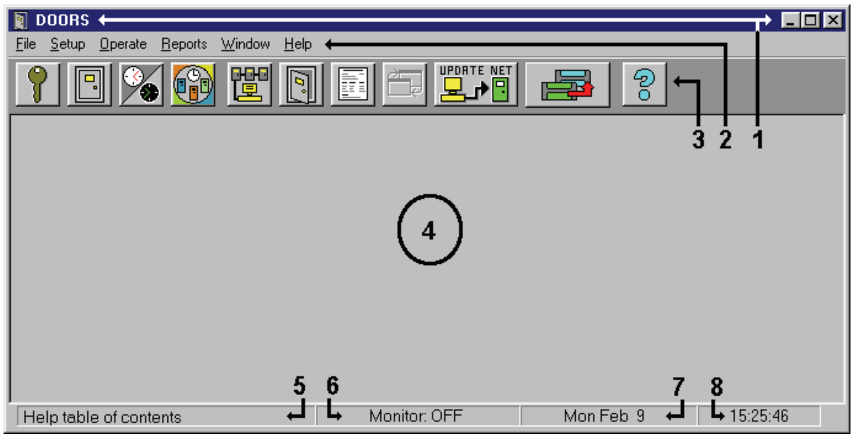


Figure 1-13: The *Doors* Desktop

1. **Window Title Bar** – On the left side of the title bar is the name of the program operating the window or the site name, if in sites mode; on the right side are the *Windows* control boxes for minimizing or maximizing the window and for immediately closing the program (refer to *Windows*' online help for information on using these boxes).
2. **Menu Bar** – A list of the pull-down menus in the *Doors* program is displayed on the menu bar. The menu bar is used for accessing all programming and configuration tasks. Sections in this manual provide all the details for using all the commands in the menu bar. Each pull-down menu option has an underlined letter. To quickly open a menu option, press the ALT key followed by the underlined letter. Sub-menus also have underlined letters and can be accessed in a similar manner. For example, to access the Setup ⇒ System pull-down menu option press **ALT S S**. If you already have the menu option opened or minimized, using the ALT key shortcut will have no effect.
3. **Tool Bar** – The tool bar is a set of tool buttons for the most used functions in the *Doors* program. Clicking on a tool button immediately opens a function's window. A summary of what functions are available on the tool bar appears in Figure 1-14 on page 22 of this section. If you have a window opened or minimized, the tool button will be greyed out and clicking on it will have no effect.
4. **Task Field** – When a task is begun by a selection from the menu bar or the tool bar, a window will appear within this field to manage whatever is necessary to perform this task. Multiple task windows can be open simultaneously within the task field. Each window in the task field will have its own title bar identifying the window. The title bar of the active task in the task field is highlighted.
5. **Status/Help Box** – The status/help box provides a brief description of the active task in the task field.
6. **Monitor Indicator Box** – The monitor indicator box displays if the system monitor is OFF or if it is ON, indicating real-time data collection of events from the access control network is being done by the *Doors* program.
7. **Date Box** – The date box displays the date kept by the host computer.
8. **Time Box** – The time box displays the time kept by the host computer (based on a 24-hour clock).

12.2 The Tool Bar

The tool bar is a collection of tool buttons for the most used functions in the *Doors* program (see Figure 1-14). Clicking on a tool button immediately opens a function's window. Placing the mouse cursor on top of a tool button displays the name of that button beside the mouse cursor.

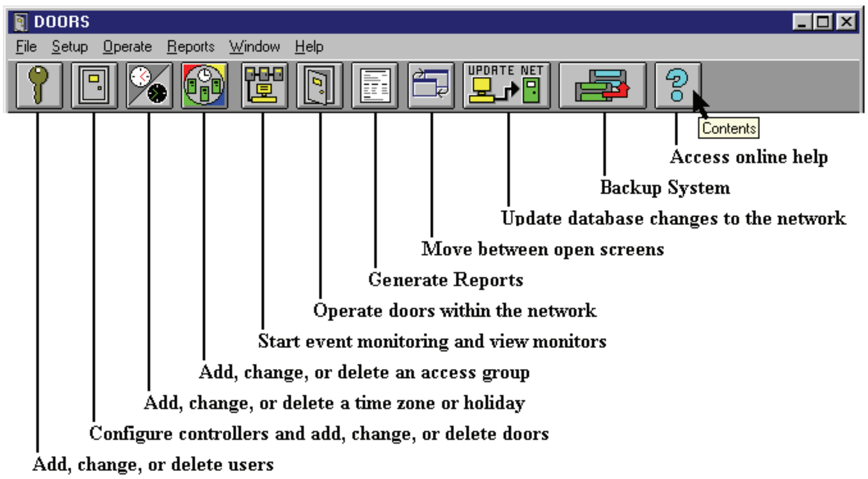


Figure 1-14: The Tool Bar

12.3 Online Help

Online help is built into the *Doors* program. To access online help, click on the [?] on the tool bar or click on Help ⇒ Contents. A new window appears placing assistance for using the *Doors* program at your fingertips.

Contents Tab

Use the contents tab when you know what section of the Users Guide contains the information you are looking for. When you double-click on the section title, all the sections that fall in that category are revealed. Double-click on the desired section and it will appear in the view screen on the right.

Index Tab

Use the index tab when you are unsure of where the information you need is located within the Users Guide. There are two ways to use the index tab:

- Scroll through the list of topics until the desired topic is found. Double-click on the topic and it will appear in the view screen on the right.
- In the space provided at the top of the listing, type in the keyword you are looking for. You are immediately taken to that point in the topics list where you may double-click on the desired topic and it will appear in the view screen on the right.

When you are finished using the online help, close it by clicking on the [X] box in the upper-right corner of the help window.

NOTE: When using online help, you may consider resizing the Doors program window to take up half of the computer screen and then resizing the online help to take up the other half of the computer screen (see Figure 1-15). This allows you to jump back and forth between the program and the online help, tracking down assistance for nested items.

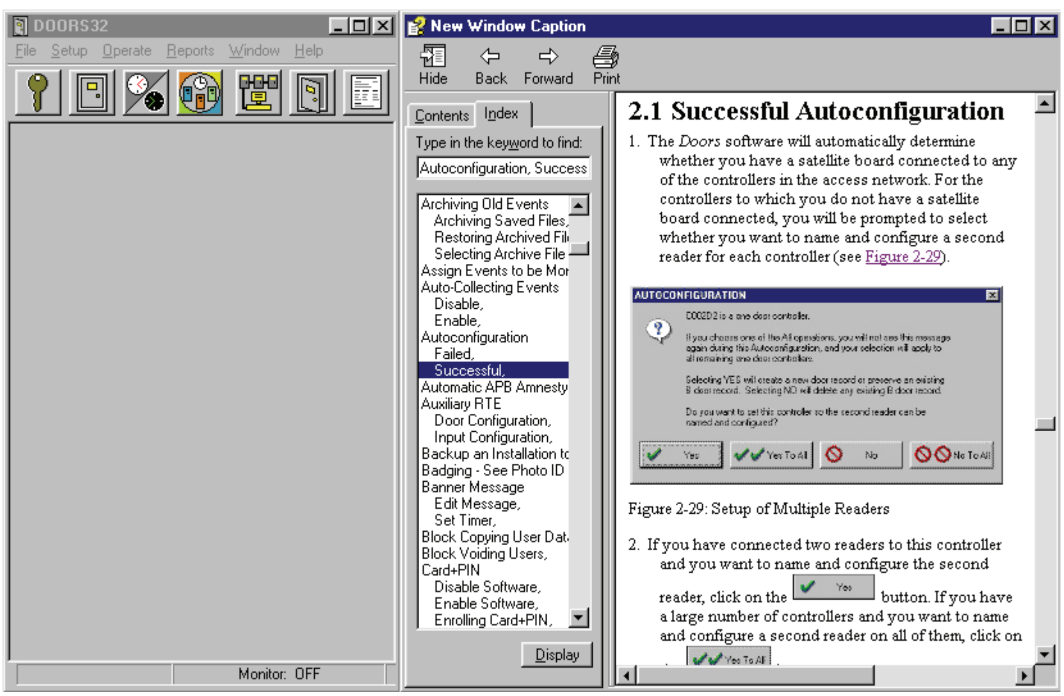


Figure 1-15: Split Screen Displaying Both *Doors* and Online Help

12.4 Exiting a *Doors* Window

Whenever changes are made to information in a window, these changes must be saved by clicking on the SAVE button before exiting the window, or the changes will be lost and must be re-entered. Once saved, the access control network must be updated for this new information to be applied by the access control network. Click on the UPDATE NET button on the tool bar to update the network (for details on the update process refer to “Update the Network” on page 35 in section 5).

1. To exit any window in the program at any time, click on the ☒ box in the upper-right corner of a window.

NOTE: If you click on the ☒ box in the upper-right corner of the main Doors window you will close the Doors program immediately, provided all changes have been saved and you have been granted operator authority to close the program.

2. If changes have been made to the database that have not been saved, a “Data Has Changed” warning will appear (see Figure 1-16).

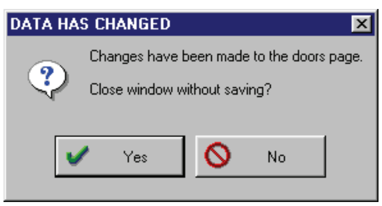


Figure 1-16: Data Has Changed Warning

3. If you still want to close the window without saving the changes, click on the Yes button.
4. If you want to save the changes before closing, click on the No button. Then click on the SAVE button.

13.0 Window Management

At times an operator might find it necessary or advantageous to have several database windows open at the same time. There are 5 tools to help in switching between open database windows.

- cascade windows
- tile windows
- tile windows horizontally
- arrange icons
- cycle windows

13.1 Cascading Windows

Cascading windows automatically takes all open windows and arranges them, one on top of another, with the title bars showing for each window.

1. To cascade all open windows, click on the Window ⇒ Cascade pull-down menu option. The individual open database windows will be organized in the *Doors* window as shown in Figure 1-17.

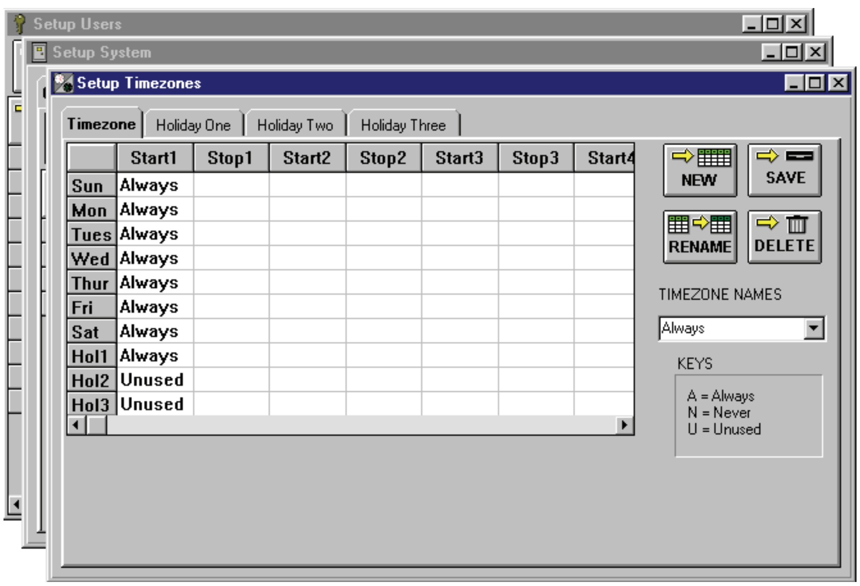


Figure 1-17: Cascading Database Windows

13.2 Tiling Windows

Tiling windows automatically takes all open windows and arranges them, side-by-side, from left-to-right, filling the *Doors* window.

1. To tile all open windows, click on the Window ⇒ Tile pull-down menu option. The individual database windows will be organized in the *Doors* window as shown in Figure 1-18.

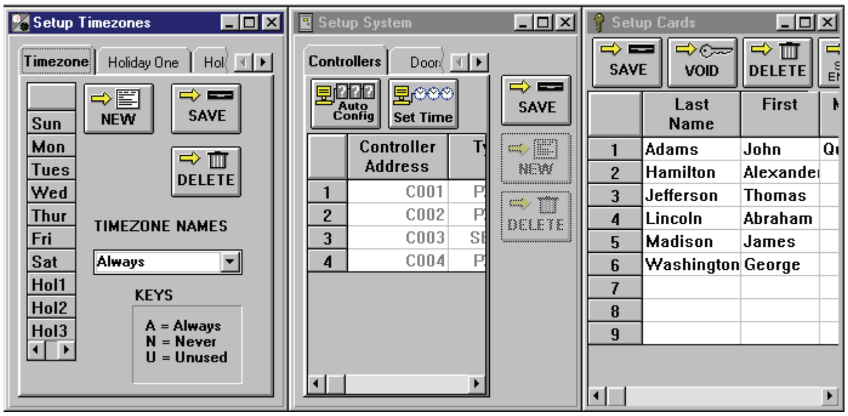


Figure 1-18: Tiled Database Windows

13.3 Tiling Windows Horizontally

Horizontally tiling windows automatically takes all open windows and arranges them, side-by-side, from top-to-bottom, filling the *Doors* window.

1. To horizontally tile all open windows, click on the Window ⇒ Tile Horizontally pull-down menu option. The individual database windows will be organized in the *Doors* window as shown in Figure 1-19.

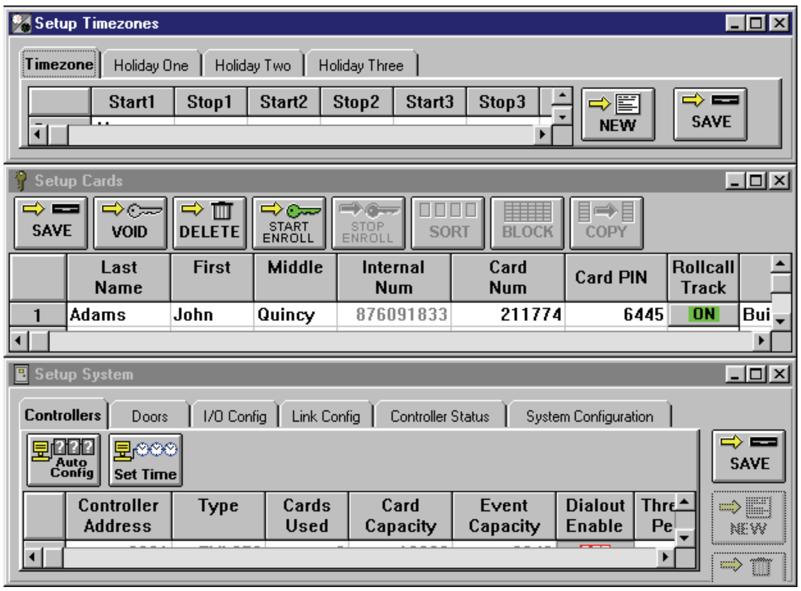


Figure 1-19: Horizontally Tiled Database Windows

NOTE: The Tile Horizontally option can only be used with 3 or fewer open windows. If there are four or more open windows, selecting the Tile Horizontally option will make the windows appear the same as selecting the Tile option.

13.4 Arranging Icons

Database windows on the *Doors* window can be reduced to icons that sit on the bottom of the *Doors* window.

1. To reduce a database window to an icon, click on the box in the upper-right corner of the database window. The individual database windows will be organized in the *Doors* window as shown in Figure 1-20.



Figure 1-20: Window Icons

2. To return the database window to its full size, click on either the box or the box in upper-right corner of the database window. The database window will return to full size.

13.5 Cycling Windows

Cycling windows allows the operator to quickly switch between all open windows.

1. To cycle between all open windows, click on the Window ⇒ Cycle pull-down menu option or click on the  icon on the tool bar. The active database window's title bar will be highlighted. If the cascade option is in use, the active database window will jump to the front of all the open windows. Each click on the  icon will switch to the next open window (see Figure 1-21).

NOTE: Cycling windows will not work if the windows are minimized as shown in "Arranging Icons" on page 28 of this section.

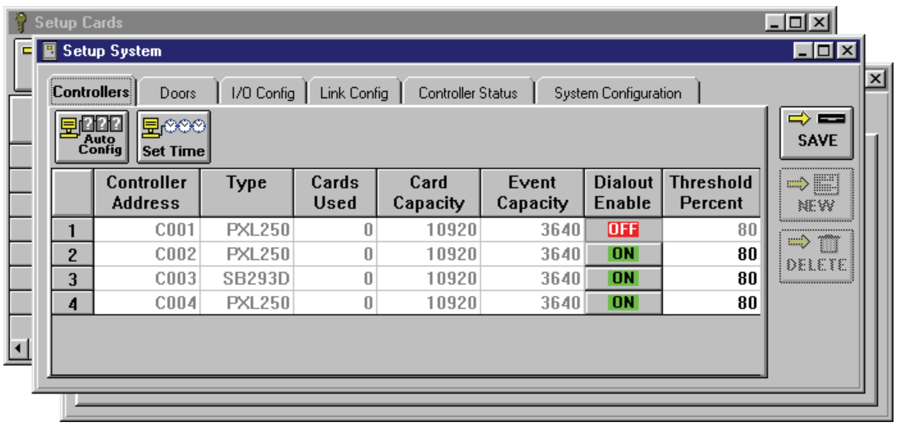


Figure 1-21: Cycling Database Windows

14.0 Retrieving the Software Revision and Logged Operator

At times it is necessary to verify the revision of the *Doors* software and to verify which operator is logged on the program.

1. To determine which version of *Doors* software is installed on the host computer and which operator is logged into the *Doors* program, click on the Help ⇒ About pull-down menu. A window similar to Figure 1-22 will appear.



Figure 1-22: Retrieving the Software Revision and Logged Operator

2. Displayed in this window is the software revision (3.76 for this example) and the current operator (for this example it is the default operator Keri).

3. Once this information has been retrieved, click on the  button to close the window.

15.0 Disconnect from the Access Control Network

In order to perform the following functions, the host computer must be actively connected to the access control network. In the case of modem connections between a host computer and a remote site, *Doors* will automatically dial-up the remote site. When these actions are complete, *Doors* does not automatically disconnect[1].

- Autoconfig
- User Enrollment (when using the Presenting to a Reader method of enrollment)
- Set Time
- Update Net
- User Initiated Door Commands
- Monitor or Event Collection Modes

NOTE: If the connection between host computer and access control network is made via modem over a distance that requires a toll call, the connection must be manually disconnected. Otherwise, the resulting phone bill can be needlessly high.

1. To disconnect from the access control network, click on the Operate ⇒ Net Disconnect pull-down menu. The access control network is immediately disconnected from the host computer.

16.0 Exiting *Doors*

Perform the following step to exit the *Doors* program and return to the operating system.

NOTE: Exiting the Doors program does not halt operation of the access control network. The network operates based on all the information uploaded to the network by the Doors program. The Doors program is only needed for making changes to the network, receiving events from the network, and for real-time monitoring of network activity.

1. Click on the File ⇒ Exit pull-down menu. If the program is connected to the access control network it will disconnect from the network. If any database changes have been made that have not been saved, the program will prompt the operator to either save or not save these changes. The *Doors* program will then shut-down.

1. When using the internal modem on the EntraGuard Gold Telephone Entry Controller, *Doors* is automatically disconnected.

End of Section.

Section 2

Set System Parameters and Verify Network Communication

The Set System Parameters and Verify Network Communication section describes the process for configuring the *Doors* communication parameters to meet those of the host computer and then verifying that basic communication is indeed happening between the host computer and all the controllers on the access control network.

The following topics are covered in this section:

- Set System Parameters
- Autoconfiguration
- Set Controller Date And Time
- Network Update
- Get Controller Status
- Set the Spreadsheet Font
- Setup Operators

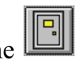
Document Number 01914-002, Revision 5.5 – July, 2005

1.0 Set the System Parameters

It is necessary to set the system parameters in order to let *Doors* know what features will be used for this network. All three of the following tasks must be performed to properly set the system parameters.

- set the network configuration parameters
- set the system option parameters
- save the system parameters

All three of these tasks are performed from the Setup System window. To access the Setup System window:

1. Click on the Setup ⇒ System pull-down menu or click the  button on the tool bar.
2. The first time the setup menu is entered (and every time until the system configuration parameters have been saved), the Setting Up The System window appears as a reminder that the system autoconfiguration needs to be performed (see Figure 2-1).

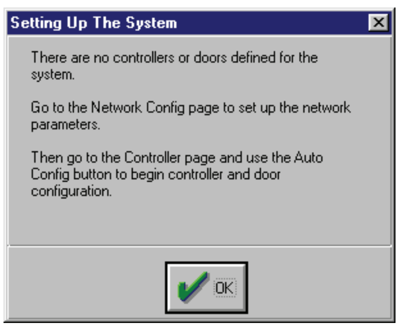


Figure 2-1: Setting Up The System Window

3. Click on the  button. The Setup System window appears (see Figure 2-2).

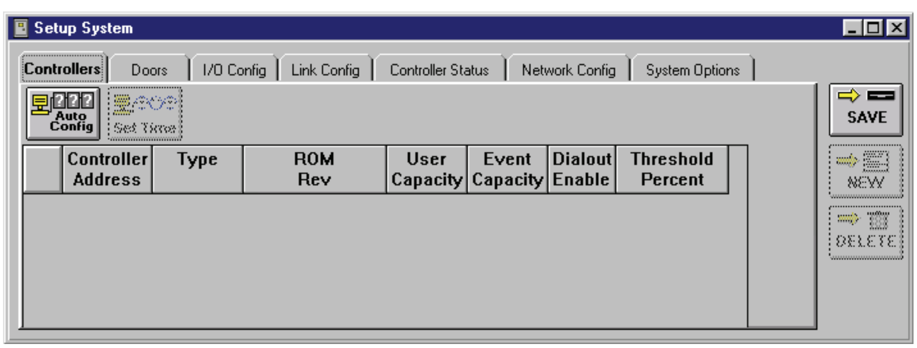


Figure 2-2: Setup System Window

1.1 Set the Network Configuration Parameters

The following network configuration parameters need to be set for proper communication between host computer and access control network.

Either
- COM port, including modem parameters

Or

- Ethernet TCP/IP

NOTE: For information regarding configuration parameters of a system that uses an EntraGuard controller, please refer to "EntraGuard" on page 1 in section 10.

1.1.1 Set the COM Port and Modem Parameters

If the system is using the computer's COM port for communication with the access control network, either through direct connect or through a modem, perform the following steps.

1. From the Setup System window, click on the **Network Config** tab. The Network Configuration window appears (see Figure 2-3).

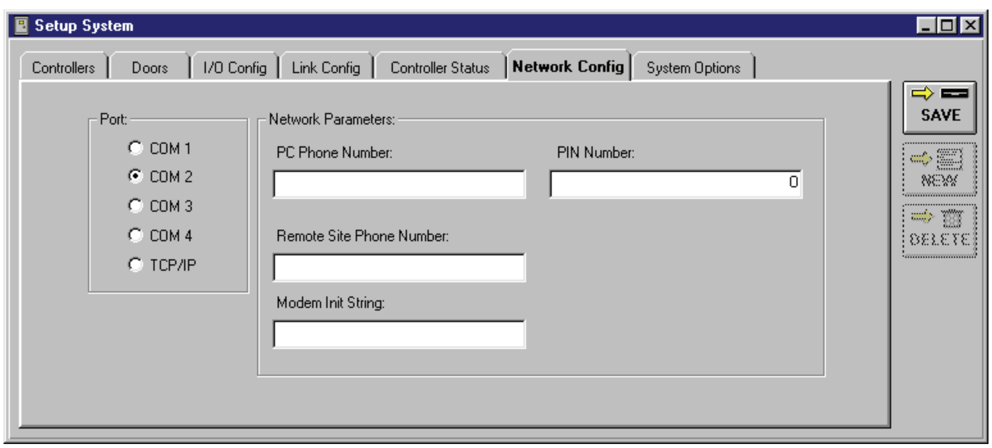


Figure 2-3: Network Configuration Tab

2. Click on the COM port radio button (**1**, **2**, **3**, or **4**) corresponding to the computer's COM port that will be used for communication between the host computer and the access control network. This will be either the COM port to which a direct serial connection or external modem is connected, or the COM port to which an internal modem is installed. Figure 2-3 shows COM port 2 enabled.

If the connection between access control network and host computer is made directly, skip to step 7. However, if the connection is made through a modem, modem parameters must be entered.

3. Click in the "PC Phone Number" field (see Figure 2-3), and enter the phone number for the modem attached to the host computer.
4. If the site should be assigned a Personal Identification Number (PIN), click on the "PIN Number" field and enter the PIN to be used for the remote site. This is an optional field.

*NOTE: Once a PIN has been assigned to a site, an operator must know that site's PIN to be able to access that site. This is an extra security measure to ensure that an operator has authorization to access any given site. When a PIN has been assigned to a site, it is stored in the software and is visible each time you open the **Network Config** tab.*

5. In most cases the modem's default initialization string (which is programmed into the modem) meets the needs of the *Doors* program and no information needs to be entered into this field. If the modem requires a special modem initialization string, click on the "Modem Init String" field and enter the modem initialization string for the PC's modem. As the modem initialization string differs per modem type and manufacturer, refer to the modem's manual for the initialization string.
6. Click on the "Remote Site Phone Number" field and enter the phone number for the modem attached to the master controller at the remote site.
7. Click on the 

button to save these changes. If the COM port and modem parameters are not saved before clicking any other button or exiting the system setup window, the data entered is lost and must be re-entered.

1.1.2 Ethernet TCP/IP Parameters

If you are using a LAN (either LAN-50, LAN-100, or LAN-500) Ethernet Converter to communicate between the host computer and the access control network, you must first install the LAN on the network. See the LAN-50 Ethernet Communication Application Note (P/N 01881-003), the LAN-100 Ethernet Communication Application Note (P/N 01881-001), or the LAN-500 Ethernet Communication Application Note (P/N 01922-001) for information on how to install the LAN. Once you have the LAN installed, you must configure *Doors*.



NOTE: A system or network administrator will be required to provide some of the necessary information for setup of the LAN.

1. From the Setup System window, click on the **Network Config** tab. The Network Configuration window appears (see Figure 2-3 on page 4 of this section).
2. Click on the **TCP/IP** radio button. The Network Configuration window will add new fields for configuring the LAN-100 (see Figure 2-4).

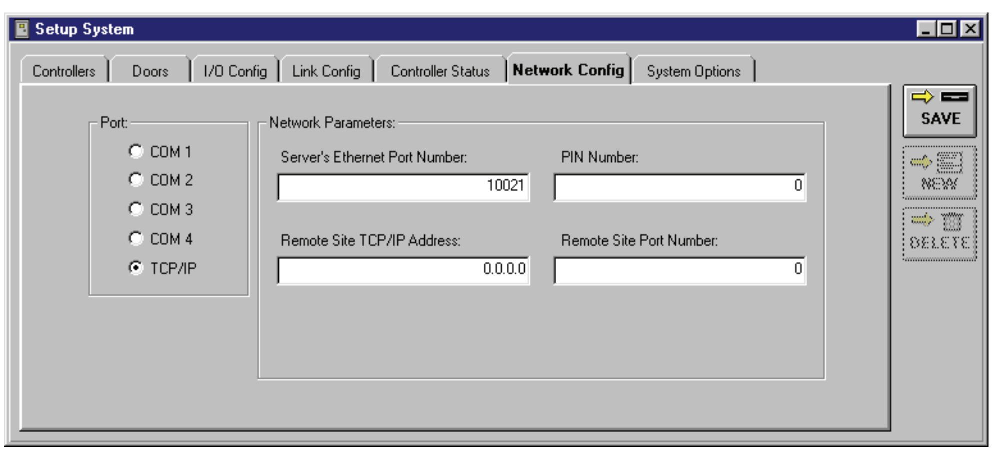


Figure 2-4: Network Configuration Tab With TCP/IP Selected

3. Click in the “Server’s Ethernet Port Number” field to enter the number assigned to the computer running *Doors*. The default is set at 10021, but will need to be changed if it conflicts with another device on the computer. **Please consult with your network administrator before making any changes**.
4. Click in the “Remote Site TCP/IP Address” field and enter the address of the LAN-100 unit. The address must be entered in the standard “dot” notation (e.g. 0.0.0.0).
5. If the site should be assigned a Personal Identification Number (PIN), click on the “PIN Number” field and enter the PIN to be used for the remote site. This is an optional field.

NOTE: Once a PIN has been assigned to a site, an operator must know that site’s PIN to be able to access that site. This is an extra security measure to ensure that an operator has authorization to access any given site. When a PIN has been assigned to a site, it is stored in the software and is visible each time you open the ***Network Config*** *tab.*

6. The Remote Site Port Number default is set at 0. This number will vary depending on whether a LAN-50 or LAN-100 is being used. Consult your systems or network administrator before changing this number.
7. Click on the 

button to save these changes. If the Ethernet TCP/IP parameters are not saved before clicking any other button or exiting the System Setup window, the data entered is lost and must be re-entered.

1.2 Set the System Option Parameters

The following system option parameters need to be set for proper system operation.

- Sites
- Badging
- EntraGuard
- Network Master Parameters
- Local Anti Passback
- Door Type (elevator/gate control)
- User Data File Export/Import
- Rollcall/Track
- Card+PIN (P-650)
- Alarm Control
- Temp Users
- Dual Verification
- Video

1. From the Setup System window, click on the **System Options** tab. The System Options window appears (see Figure 2-5).

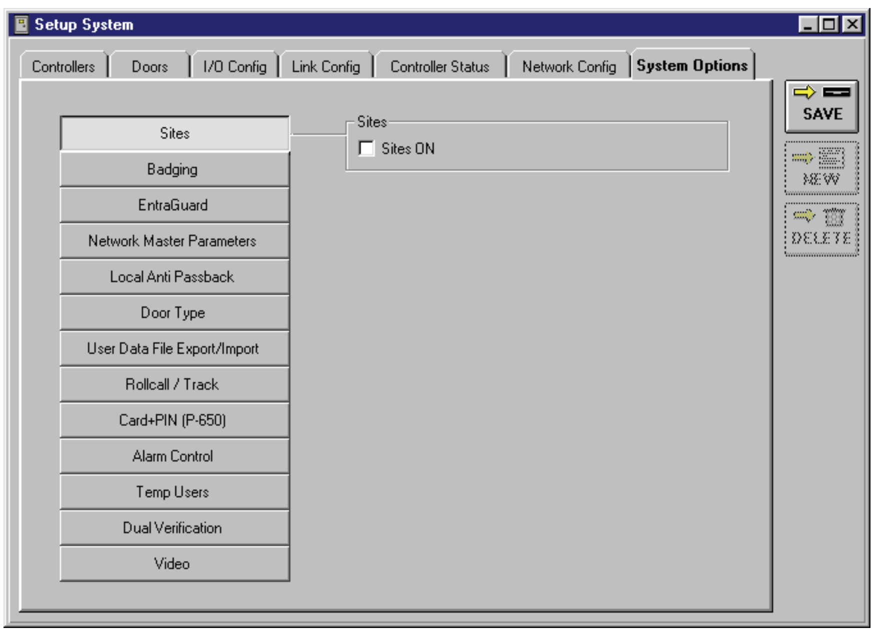


Figure 2-5: System Options Tab

1.2.1 Set Sites

See "Multiple Sites" on page 1 in section 8 for a complete description of how to enable, use, and disable the multiple sites feature in *Doors*.

The Sites parameter allows an operator to enable or disable the multiple sites feature of the *Doors* program.

The program default is for Sites to be OFF.

1. If the Sites ON field is not already visible on the System Options tab, click on the 

button. The System Options window will reveal the field for enabling multiple sites (see Figure 2-5 on page 7 of this section).
2. If your application does not use multiple sites, verify there is **not** a check mark in the Sites ON box.
3. To enable multiple sites mode, click in the check box beside the Sites ON field. When there is a check in the box, the feature is enabled. To disable this field, click in the check box again and remove the check mark (this is the default value).

NOTE: A number of changes are made to the access control databases when multiple sites mode is enabled. These changes add the fields necessary to manage multiple sites. For simplicity in explaining the features in the Doors program, the majority of this Users Guide assumes that multiple sites mode is not enabled. Multiple site features are explained in "Multiple Sites" on page 1 in section 8.

1.2.2 Set Badging

For information regarding badging, please refer to "Photo Badge Management" on page 1 in section 9.

Badging is a separate feature of the *Doors* access control software. Badging is not fully active until a License Code is obtained from the Keri Systems' Customer Support department. To support the software used for badging, a fee is charged for this License Code. A demonstration version can be installed if desired. Before installation, please refer to the badging requirements found in "Photo Badge Management Requirements" on page 6 in section 1 to ensure your host computer is capable of running the badging feature.

1.2.3 Set EntraGuard

See "EntraGuard" on page 1 in section 10 for a complete description of how to enable, use, and disable the EntraGuard feature in *Doors*.

The EntraGuard parameter allows an operator to enable the telephone entry feature of the *Doors* program for use with an EntraGuard Telephone Entry controller.

The program default is for EntraGuard to be OFF.

1. From the System Options tab, click on the [EntraGuard] button. The System Options window will reveal the EntraGuard field where options concerning use of an EntraGuard controller may be set (see Figure 2-6).

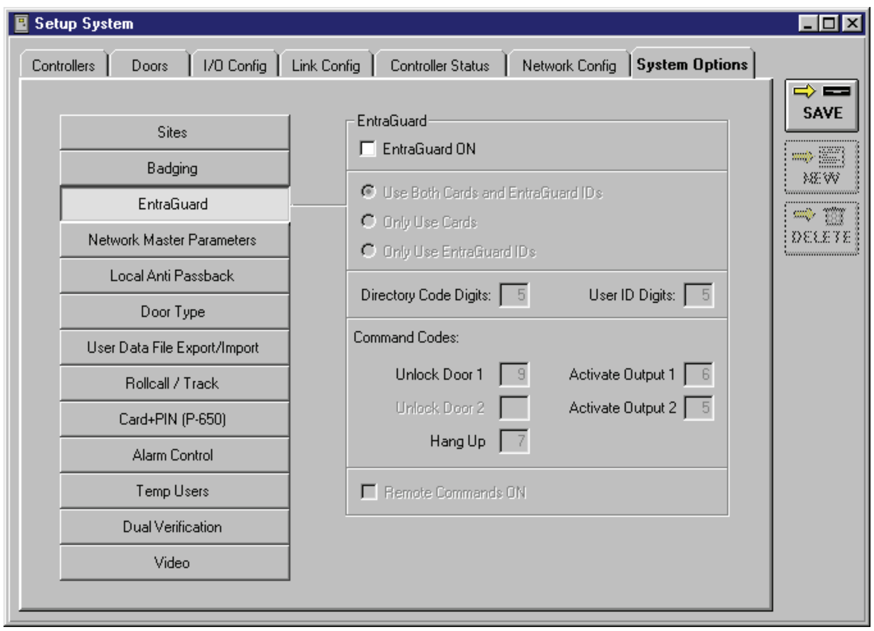


Figure 2-6: EntraGuard Entry Field

2. If your system is not using an EntraGuard controller, verify there is **not** a check mark in the EntraGuard ON box (see Figure 2-6).
3. To enable use of an EntraGuard controller, click in the check box beside the EntraGuard ON field[1]. When there is a check in the box, the feature is enabled. To disable this field, click in the check box again and remove the check mark (this is the default value).

NOTE: Before disabling the EntraGuard feature, make sure there is no check in the Remote Commands ON check box and there are no EntraGuard units connected to the network.

NOTE: A number of changes are made to the access control databases when EntraGuard mode is enabled. These changes add the fields necessary to manage an EntraGuard controller. For simplicity in explaining the features in the Doors program, the majority of this Users Guide assumes that EntraGuard entry mode is not enabled. EntraGuard related features are explained in detail in "EntraGuard" on page 1 in section 10.

1. The EntraGuard feature is automatically enabled if an EntraGuard unit is detected when an autoconfiguration is performed on the system.

1.2.4 Set Network Master Parameters

The following network master parameters, when set, apply to all controllers on the access control network:

- daylight savings adjustment
- global unlock enable
- global lock enable
- global secure time

1. From the System Options tab, click on the 

button. The System Options window will reveal the Network Master Parameters field where the three parameters listed above may be set (see Figure 2-7).

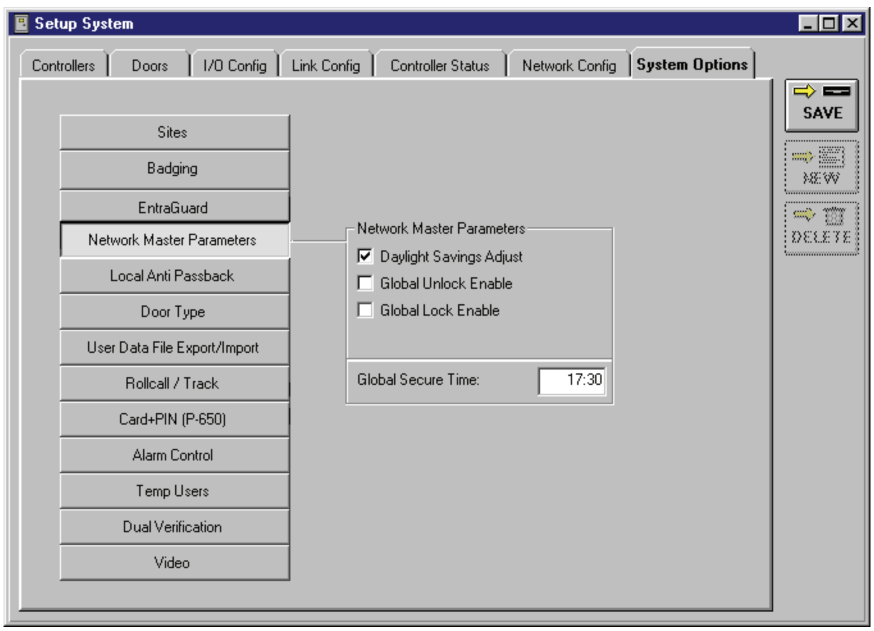


Figure 2-7: Network Master Parameters Field

1.2.4.1 Daylight Savings Adjustment

The Daylight Savings Adjustment feature allows the controllers to automatically adjust the time on the controllers when daylight savings time comes and goes.

1. To enable the daylight savings adjustment click in the check box beside the Daylight Savings Adjust field. When there is a check in the box, the feature is enabled (this is the default value).
2. To disable this field, click in the check box again and remove the check mark.

NOTE: Daylight Savings Time for all participating U.S. states, the District of Columbia, and U.S. possessions begins at 2 A.M. on the first Sunday in April and ends at 2 A.M. on the last Sunday in October. For states and countries not participating in daylight savings time, you must disable the daylight savings time adjustment feature.

1.2.4.2 Global Unlock Enable

The global unlock enable feature allows the general purpose input of the master controller to be used to automatically unlock all online and functioning doors in the access control network (refer to the PXL-250 Tiger Controller and SB-293 Technical Reference Manual - P/N 01836-004, the PXL-250 Quick Start Guide - P/N 01835-002, or the PXL-500 Quick Start Guide - P/N 01918-001 for general purpose information).

1. To enable the global unlock enable feature click in the check box beside the Global Unlock Enable field. When there is a check in the box, the feature is enabled.
2. To disable this field, click in the check box again and remove the check mark (this is the default value).

NOTE: The global unlock enable feature is not fire marshall approved. Check your local codes for fire safety management.

NOTE: Global Unlock takes precendence over ALL other lock or unlock commands. Any attempt to Restore an Auto Unlock/Lock time zone while the Global Unlock is active will be ignored by the master controller.

NOTE: Global unlock enable is disabled on the master controller if the master controller uses the Auxiliary Request to Exit feature.

1.2.4.3 Global Lock Enable

The global lock enable feature allows the general purpose input of the master controller to be used to automatically lock all online and functioning doors in the access control network. Global Lock specifically uses Input 4 on an SB-593 Satellite board attached to the master controller.

1. To enable the global lock enable feature click in the check box beside the Global Lock Enable field. When there is a check in the box, the feature is enabled.
2. To disable this field, click in the check box again and remove the check mark (this is the default value).

NOTE: The global lock enable feature is not fire marshall approved. Check your local codes for fire safety management.

NOTE: Global Lock takes precendence over ALL other lock or unlock commands EXCEPT for Global Unlock. Any attempt to Restore an Auto Unlock/Lock time zone while the Global Lock is active will be ignored by the master controller.

NOTE: Global lock enable is disabled on the master controller if the master controller uses the Auxiliary Request to Exit feature.

1.2.4.4 Global Secure Time

The global secure time allows an operator to define a time of day when all doors that have been manually unlocked (see “Unlock Doors” on page 8 in section 6) should be locked. The global secure time ensures that all doors are locked at least once a day. Global secure is not applied to doors that have been assigned a time zone; these doors are unlocked/locked per the time zone stop/start times. Global Secure will not restore a suspended unlock/lock time zone (see “Suspend/Restore Auto Unlock/Lock” on page 14 in section 6). Global Unlock and Continuous RTE have precedence over Global Secure. This field cannot be disabled.

1. Click in the Global Secure Time field and enter the time when all doors that have been manually unlocked should be locked. The default value is 17:30 (5:30 P.M.).

NOTE: The global secure time is based on a 24-hour clock. For example: Midnight is entered as 00:00, 8:30 A.M. is entered as 08:30, and 11:30 P.M. is entered as 23:30.

NOTE: Once all the Network Master Parameters have been set, click on the 

button to save these changes. If the network master parameters are not saved before clicking any other button or exiting the system options window, the data entered is lost and must be re-entered.

1.2.5 Set Local Anti Passback

Anti Passback (APB) provides one-card one-way access into and then out of a secure area. It prevents someone from using a card to enter a secure area and then passing that card back to someone else to use to enter that same secure area.

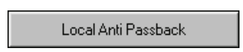
Local APB means the passback rules are applied on a per controller basis. Each controller tracks which users have been through its doors; controllers cannot track which users have been through other controllers/doors. *Doors* software uses local APB; referred to as APB for the rest of this Users Guide.

NOTE: APB is not applicable to EntraGuard controllers.

At a given controller using APB, no exit is allowed through a controller's B-reader unless entrance was made through that same controller's A-reader. No entrance is allowed through a controller's A-reader unless exit was made through that same controller's B-reader. If a user presents a card to the reader at a door, but decides not go through that door (the door is not opened), APB is **not** applied allowing the user access through that door later.

NOTE: In order for APB to properly track when a user gains access through a door, the door must have a door switch installed. Refer to the PXL-250 Tiger Controller and SB-293 Technical Reference Manual (P/N 01836-004), the PXL-250 Quick Start Guide (P/N 01835-002), or the PXL-500/PXL-510 Quick Start Guide (P/N 01918-001) for door switch installation information.

The program default is for APB to be OFF. To implement APB, the APB feature must be enabled in the software and then configured for the desired controllers and cards/users. APB amnesty can be granted to individual cards, allowing those cards to violate the APB rules. Amnesty can be automatically granted to a controller periodically (i.e. once an hour), automatically granted to a controller at a specific time each day (i.e. 02:00 hours, or 2 A.M.), or not automatically granted at all (amnesty can be manually granted by an operator to a user at any time - see "Anti Passback Amnesty" on page 26 in section 6).

1. From the System Options tab, click on the 

button. The System Options window will reveal the Local Anti Passback field where the APB options are set (see Figure 2-8).

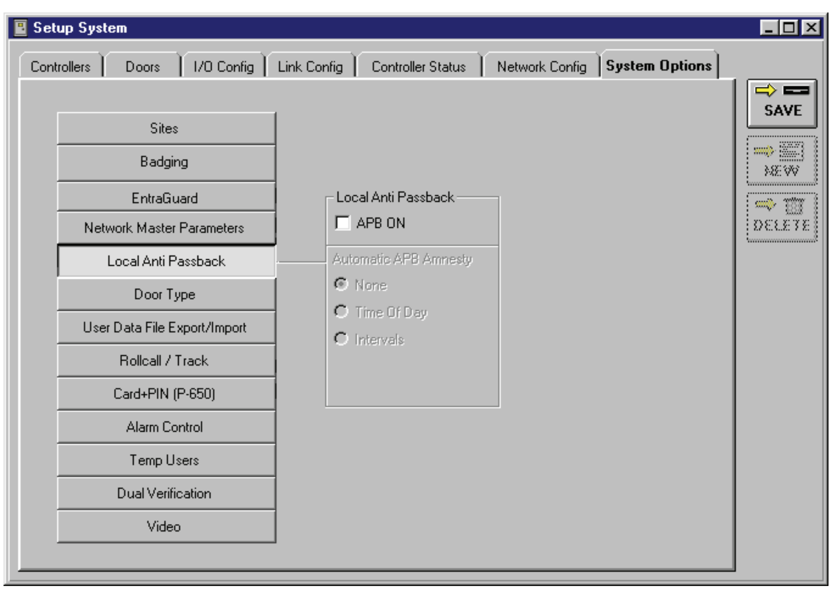


Figure 2-8: Local Anti Passback Field

2. If APB is not required in your application, verify there is **not** a check mark in the APB ON box. This is the default value (see Figure 2-8 on page 13 of this section).
3. To enable APB, click in the APB ON check box. A check mark appears in the APB ON box and the following window appears (see Figure 2-9).

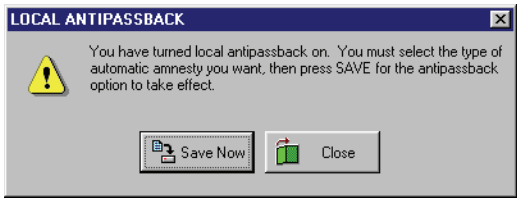


Figure 2-9: Enabling Local Anti Passback Confirmation

4. Click on the 

 button. A "Saved Configuration" window flashes on the screen and then the three types of APB amnesty appear as radio buttons displayed in the Automatic APB Amnesty field (see Figure 2-10).
5. Once an APB amnesty type has been set (see below for information on each option), click on the 

 button to save these changes. If the APB amnesty type is not saved before clicking any other button or exiting the System Options window, the data entered is lost and must be re-entered.

1.2.5.1 Automatic APB Amnesty – None

When the None radio button is ON (see Figure 2-10), it means that although APB is in use, amnesty is never automatically granted. If amnesty is ever required for a user, it can be manually granted by an operator (this process is described in "Anti Passback Amnesty" on page 26 in section 6).



Figure 2-10: No Automatic APB Amnesty

1.2.5.2 Automatic APB Amnesty – Time Of Day

Click on the Time of Day radio button to select this option. When the Time of Day radio button is ON, amnesty is automatically granted to all APB configured users at all APB configured controllers at a specific time each day. A Time of day entry window appears when the Time of Day option is selected (see Figure 2-11). Click in this field and enter the time of day when amnesty should be granted, for example, 02:00 hours (2 A.M.). The default value for this field is 00:00 (Midnight).

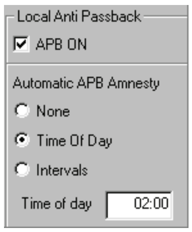


Figure 2-11: Set the Time of Day Amnesty Time

NOTE: The Time of Day amnesty time is based on a 24-hour clock. For example: Midnight is entered as 00:00, 8:30 A.M. is entered as 08:30, and 11:30 P.M. is entered as 23:30.

1.2.5.3 Automatic APB Amnesty – Intervals

Click on the Intervals radio button to select this option. When the Intervals radio button is ON, amnesty is automatically granted to all APB configured users at all APB configured controllers periodically. For instance, if the time interval is set to 01:00, amnesty will be granted every hour. An Interval window appears when the Intervals option is selected (see Figure 2-12). Click in this field and enter the time interval when amnesty should be granted, for example, 01:00 (once an hour). The default value for this field is 00:15 (or once every 15 minutes). This field may not be set for any amount of time less than 15 minutes nor more than 23:59.

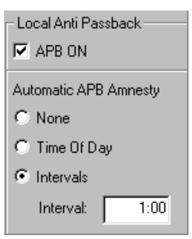


Figure 2-12: Set the Intervals Amnesty Time

NOTE: The Intervals amnesty time is based on a 24-hour clock. For example: once every 30 minutes is entered as 00:30, once every 4 hours is entered as 04:00, and once every 12 hours is entered as 12:00.

1.2.6 Disable Local Anti Passback

1. To disable APB, click in the APB ON check box. The check mark that was there disappears and the following window appears (see Figure 2-13).

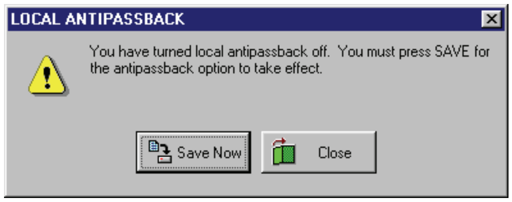


Figure 2-13: Disabling Local Anti Passback

2. Click the 

button. A confirmation window appears (see Figure 2-14).

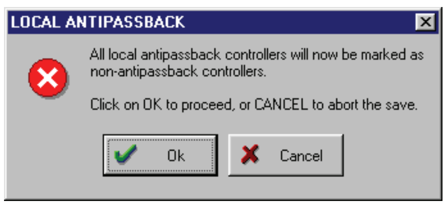
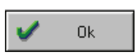


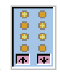
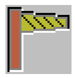
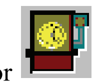
Figure 2-14: Disabling Local Anti Passback Confirmation

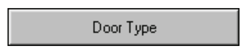
3. Click the 

button and the APB option has been disabled.

1.2.7 Set Door Type

The door type parameter allows an operator to enable the elevator, gate, and time and attendance terminal control features of the *Doors* program. When the elevator, gate, or time and attendance terminal control features are enabled, the *Doors* program makes several minor changes to support the selections.

- A Door Type column is added to the System ⇒ Setup Doors tab allowing a specific door to be identified as a door, elevator, gate, or time and attendance terminal (see "Assign a Door Type" on page 29 in section 3).
- The standard icon for doors, viewed as , changes to appear as  for doors identified as an elevator,  for doors identified as a gate, or  for doors identified as a time and attendance terminal when creating Access Groups (see "Setup Access Groups" on page 44 in section 3) or when performing manual door control (see "Lock, Unlock, Suspend and Restore Doors" on page 3 in section 6).
- An event filtering column appears in the Setup ⇒ Monitor and Events ⇒ Messages window when elevator control is enabled (see "Elevator Reports Events" on page 23 in section 5).

1. From the System Options tab, click on the 

button. The System Options window will reveal the Door Type field where selections may be made for door type control (see Figure 2-15).

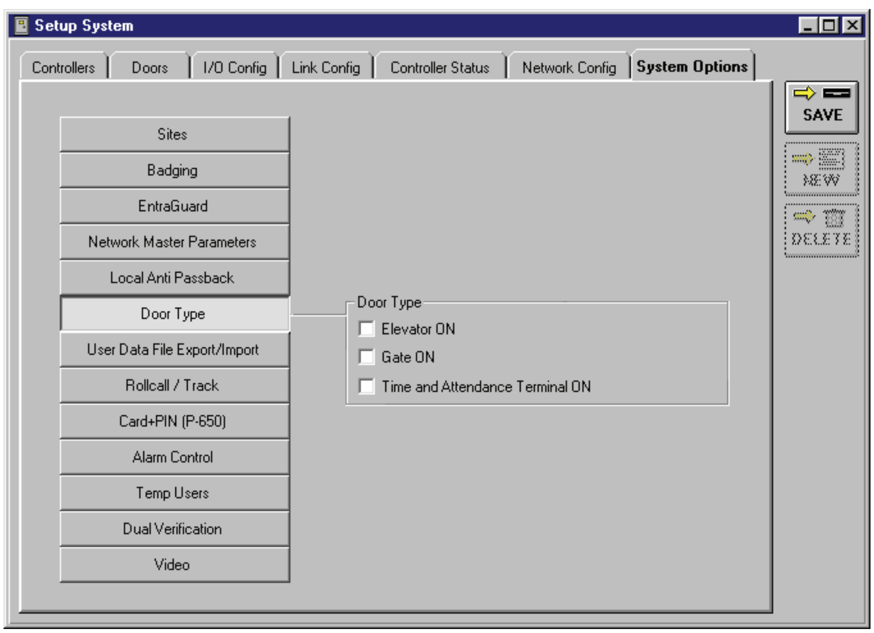


Figure 2-15: Door Type Field

2. If your application does not use elevator, gate, or time and attendance terminal control, verify there are **no** check marks in the Elevator ON, Gate ON, or Time and Attendance Terminal ON boxes. This is the default value (see Figure 2-15).

3. To enable elevator, gate, or time and attendance terminal control, click in the box beside Elevator ON, Gate ON, or Time and Attendance Terminal ON. A check mark appears in the check box and one of the following windows appear, depending on which box was checked (see Figure 2-16, Figure 2-17, and Figure 2-18).

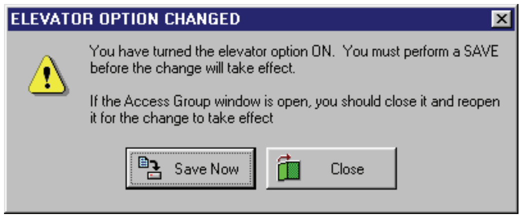


Figure 2-16: Elevator Option Changed Warning - ON

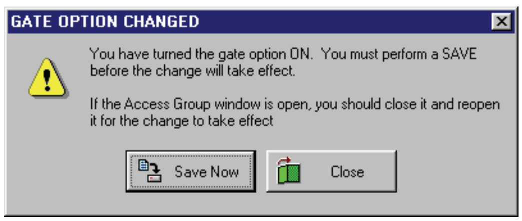


Figure 2-17: Gate Option Changed Warning - ON

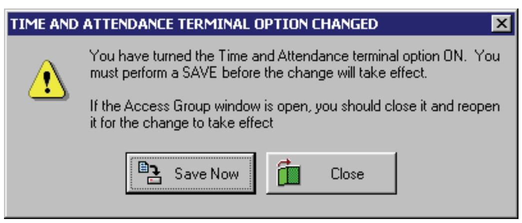
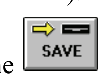


Figure 2-18: Time and Attendance Terminal Option Changed Warning - ON

4. Click on the 

button. A “Saved Configuration” window flashes on the screen.
5. You must complete this activation and saving process for each door type option you use (once for elevator, once for gate, and once for time and attendance terminal).

6. Once the Door Type field is filled out as needed, click on the 

button to save these changes. If the Door Type is not saved before clicking any other button or exiting the System Options window, the data entered is lost and must be re-entered.

1.2.8 Disable Door Type

1. To disable elevator, gate, or time and attendance terminal control, click in the corresponding check box. The check mark that was there disappears and one of the following windows appear, depending on which box was checked (see Figure 2-19, Figure 2-20, and Figure 2-21).

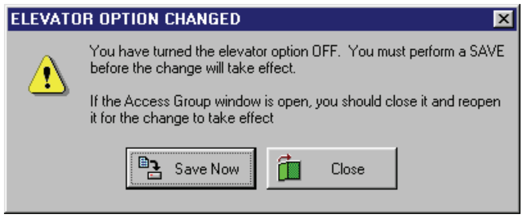


Figure 2-19: Elevator Option Changed Warning - OFF

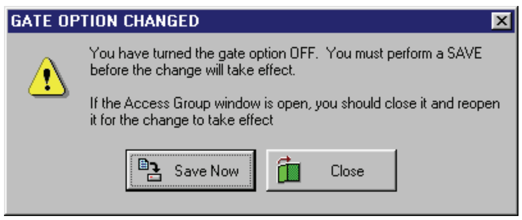


Figure 2-20: Gate Option Changed Warning - OFF

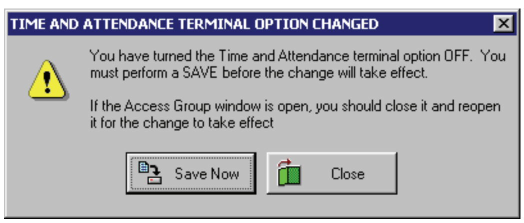


Figure 2-21: Time and Attendance Terminal Option Changed Warning - OFF

2. Click the  button. A “Saved Configuration” window flashes on the screen. You must complete the process to disable each door type individually.

3. Once the Door Type field appears as needed, click on the  button to save these changes. If the Door Type is not saved before clicking any other button or exiting the System Options window, the data entered is lost and must be re-entered.

1.2.9 Set User Data Export/Import

For detailed information, please refer to “User Data File Export/Import” on page 1 in section 11.

User Data File Export/Import is a separate feature of the *Doors* access control software. User Data File Export/Import is not fully active until a License Code is obtained from the Keri Systems’ Customer Support department. To support the software used, a fee is charged for this License Code. Before installation, please refer to the requirements found in the User Data File Export/Import Application Note (P/N 01805-001) to ensure you are properly qualified to use the User Data File Export/Import feature.

1.2.10 Set Rollcall/Track

The rollcall/track parameter allows an operator to enable the rollcall/track control feature of the *Doors* program. When the rollcall/track feature is enabled, the operator is able to view user status after collecting events or during real time Montoring.

The program default is for rollcall/track to be OFF. To implement rollcall/track, the rollcall/track feature must be enabled in the software and then activated for the desired cards/users.

1. From the System Options tab, click on the 

button. The System Options window will reveal the Rollcall/Track field where the Rollcall/Track feature may be enabled (see Figure 2-22).

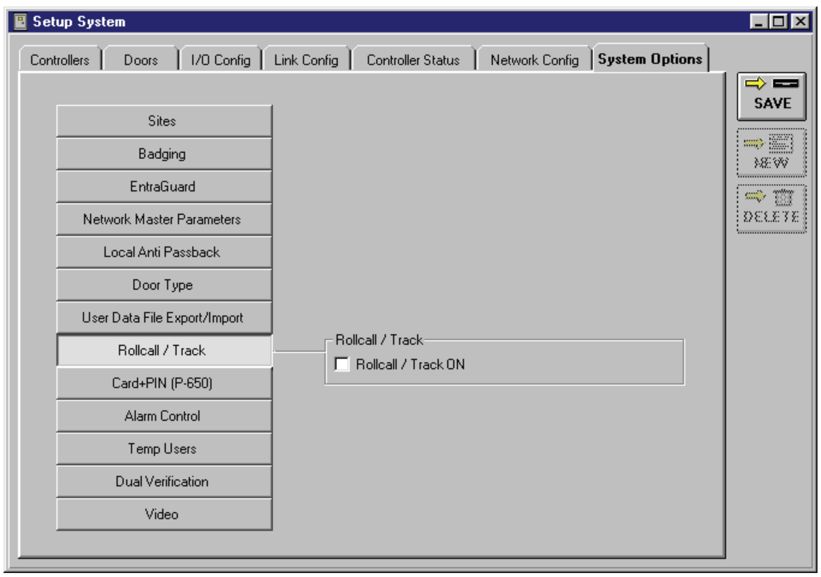


Figure 2-22: Rollcall/Track Field

2. If your application does not use rollcall/track, verify there is **not** a check mark in the Rollcall/Track ON box. This is the default value (see Figure 2-22).
3. To enable rollcall/track, click in the check box beside the Rollcall/Track ON field. A check mark appears in the check box and the following window appears (see Figure 2-23).

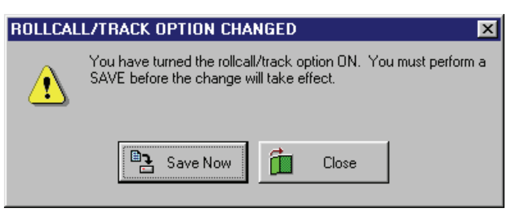
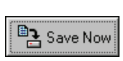


Figure 2-23: Rollcall/Track Option Changed Warning - ON

4. Click on the 

button. A "Saved Configuration" window flashes on the screen.
5. Click on the 

button to save these changes. If the Rollcall/Track changes are not saved before clicking any other button or exiting the System Options window, the data entered is lost and must be re-entered.

1.2.11 Disable Rollcall/Track

1. To disable Rollcall/Track, click in the Rollcall/Track ON check box. The check mark that was there disappears and the following window appears (see Figure 2-24).

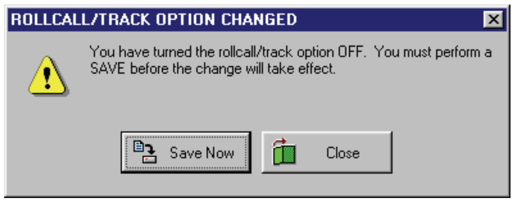


Figure 2-24: Rollcall/Track Option Changed Warning - OFF

2. Click the  button. A "Saved Configuration" window flashes on the screen.
3. Click on the  button to save these changes. If the Rollcall/Track changes are not saved before clicking any other button or exiting the System Options window, the data entered is lost and must be re-entered.

1.2.12 Set Card+PIN (P-650) Mode

NOTE: The Card+PIN (P-650) feature must be used in connection with the P-650 Card+PIN Proximity Reader and Keypad, PXL-250W controller, and 26-bit Wiegand access cards to provide a secondary method of user identification tied to the card itself. Enrollment of cards must be done by block enrollment (see "Block Enrollment by Card Number Range" on page 3 in section 4). If a card is lost, it should be voided from the system immediately.

The Card+PIN (P-650) parameter allows an operator to view the PIN associated with each access card. The Card PIN (Personal Identification Number) is a special number automatically generated and assigned to a card during enrollment when the P-650 is in use. This PIN allows a secondary verification of a user by requiring a PIN be entered after presenting a valid access card. The Card PIN cannot be changed or edited and must be given to the user with the card.

The program default is for Card+PIN (P-650) to be OFF. In order to view the Card+PIN (P-650) column in the Setup Users window, the Card+PIN (P-650) feature must be enabled in the software.

1. From the System Options tab, click on the 

button. The System Options window will reveal the Card+PIN (P-650) field (see Figure 2-25).

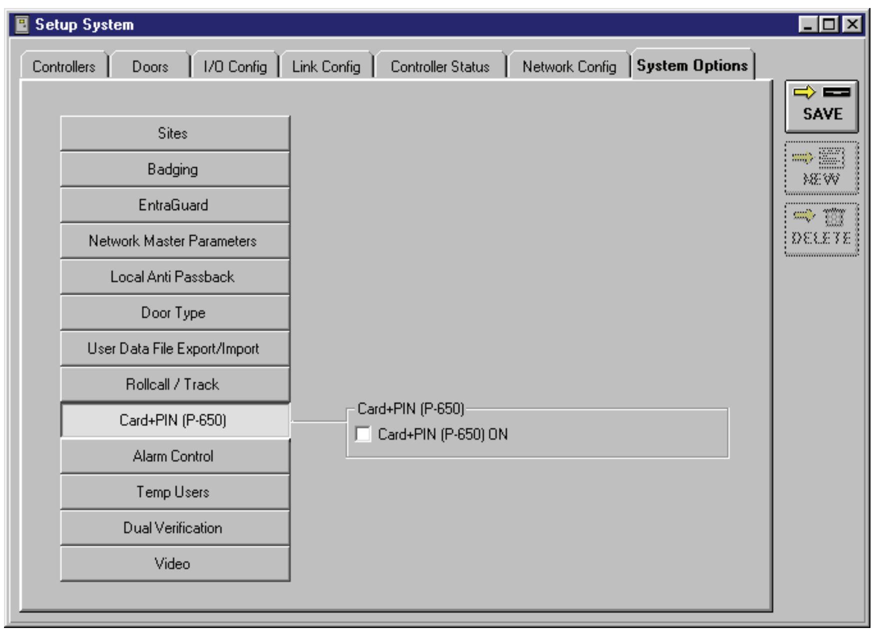


Figure 2-25: Card + PIN (P-650) Field

2. If your system is not using a P-650 Card+PIN Proximity Reader and Keypad, verify there is **not** a check mark in the **Card+PIN (P-650) ON** box. This is the default value (see Figure 2-25).

NOTE: The system will automatically generate a card PIN number for each card during enrollment. The Card+PIN (P-650) feature is only supported for the 26-bit Wiegand formatted card. PINs displayed for other card formats are not valid PIN numbers and will not work on the P-650 reader.

3. To enable the Card+PIN (P-650) feature, click in the check box beside the **Card+PIN (P-650) ON** field. A check mark appears in the check box and the following window appears (see Figure 2-26 on page 23 of this section). When there is a check in the box, the feature is enabled and you will be able to view the individual card PINs associated with each card in the User Spreadsheet window.

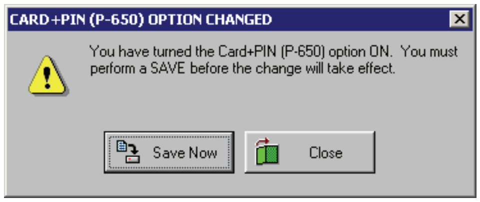


Figure 2-26: Card+PIN (P-650) Option Changed Warning - ON

4. Click the 

button. A “Saved Configuration” window flashes on the screen followed by an information window regarding the Card+PIN (P-650) feature. After reading the reminder, click on the 

button to return to the System Options tab.
5. Click on the 

button to save these changes. If the Card+PIN (P-650) changes are not saved before clicking any other button or exiting the System Options window, the data entered is lost and must be re-entered.

NOTE: The Card+PIN (P-650) column displayed in the User Spreadsheet window will not be visible if an operator has been given Read Only (RO) rights in the Setup Users category during setup of operators (see “Setup Operators” on page 45 in this section).

1.2.13 Disable Card+PIN (P-650)

1. To disable the Card+PIN (P-650) feature, click in the Card+PIN (P-650) ON check box. The check mark that was there disappears and the following window appears (see Figure 2-27).

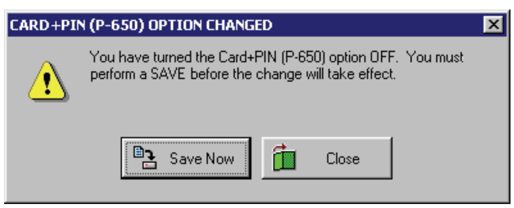


Figure 2-27: Card+PIN (P-650) Option Changed Warning - OFF

2. Click the 

button. A “Saved Configuration” window flashes on the screen.
3. Click on the 

button to save these changes. If the Card+PIN (P-650) changes are not saved before clicking any other button or exiting the System Options window, the data entered is lost and must be re-entered.

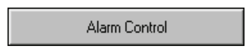
1.2.14 Set Alarm Control

See "Alarm Control" on page 1 in section 12 for a complete description of how to enable, use, and disable the Alarm Control feature in *Doors*.

The Alarm Control parameter allows an operator to enable the alarm control feature of the *Doors* program for use with a NetworX NX-8E Alarm Panel.

NOTE: In order for the Alarm Control feature to be enabled, a PXL-510 controller must be set as the master controller and connected to a NetworX NX-8E Alarm Panel. For further information on installing necessary controllers for use with the alarm control feature, refer to the PXL-500/PXL-510 Quick Start Guide (P/N 01918-001) and the NetworX NX-8E Alarm Panel Application Note (P/N 01919-001).

The program default is for Alarm Control to be OFF.

1. From the System Options tab, click on the 

button. The System Options window will reveal the Alarm Control field (see Figure 2-28).

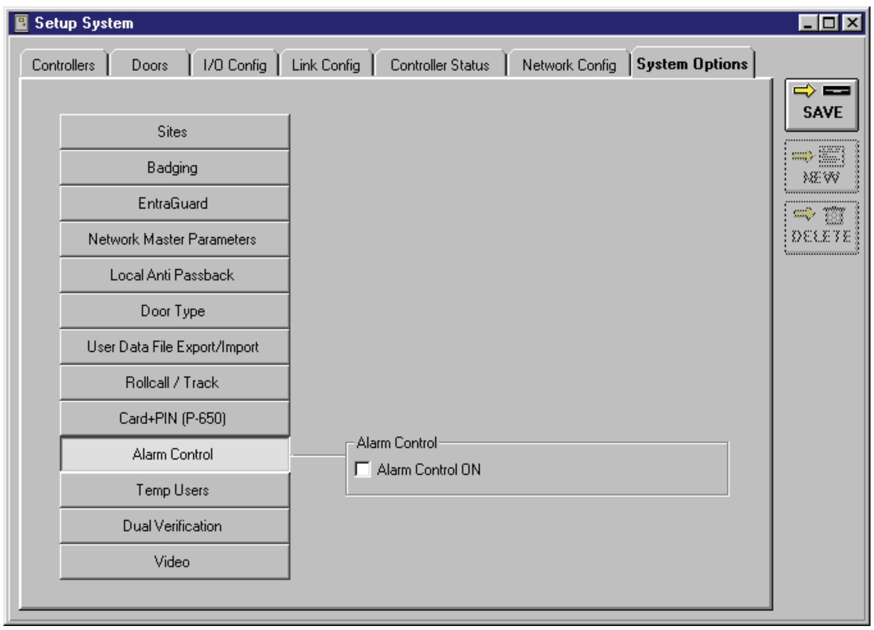


Figure 2-28: Alarm Control Field

2. If your system is not using a PXL-510 master controller connected to a NetworX NX-8E Alarm Panel, Doors will not allow the Alarm Control feature to be enabled.
3. To enable use of the Alarm Control feature in connection with a PXL-510 master controller, click in the check box beside the Alarm Control ON field. When there is a check in the box, the feature is enabled. To disable this field, click in the check box again and remove the check mark (this is the default value).

NOTE: A few changes are made to the access control databases when the Alarm Control feature is enabled. These changes add the fields necessary to manage the alarm system. For simplicity in explaining the features in the Doors program, the majority of this Users Guide assumes that the Alarm Control feature is not enabled. Alarm Control related features are explained in detail in "Alarm Control" on page 1 in section 12.

1.2.15 Disable Alarm Control

1. To disable Alarm Control, click in the Alarm Control ON check box. The check mark that was there disappears and the following window appears (see Figure 2-29).

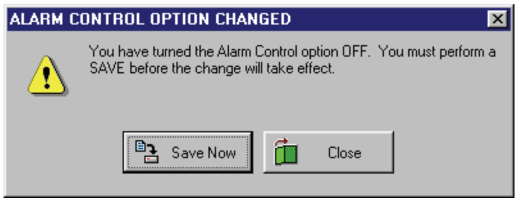


Figure 2-29: Alarm Control Option Changed - OFF

2. Click the 

button. A “Saved Configuration” window flashes on the screen.
3. Click on the 

button to save these changes. If the Alarm Control changes are not saved before clicking any other button or exiting the System Options window, the data entered is lost and must be re-entered.
4. Now click on the 

button on the tool bar and update the access control network with the new information.

1.2.16 Set Temp Users

NOTE: Enabling the Temp Users feature reduces the number of cards/User IDs that can be enrolled from 65,535 to 19,110.

NOTE: The Temp Users feature is for use on a PXL-500 controller only. Although a combined PXL-500/ PXL-250 network is possible, the Temp Users feature will work only on the PXL-500 controlled doors.

See “Temp Users” on page 1 in section 13 for a complete description of how to enable, use, and disable the Temp Users feature in *Doors*.

The Temp Users parameter allows an operator to enable or disable the Temp Users feature of the *Doors* program. Enabling the Temp Users feature allows an operator to set a future date and time for activation and expiration of a credential.

Since enabling the Temp Users feature greatly reduces the number of cards that may be enrolled, the program default is for Temp Users to be OFF.

1. From the System Options tab, click on the 

button. The System Options window will reveal the Temp Users field (see Figure 2-30).

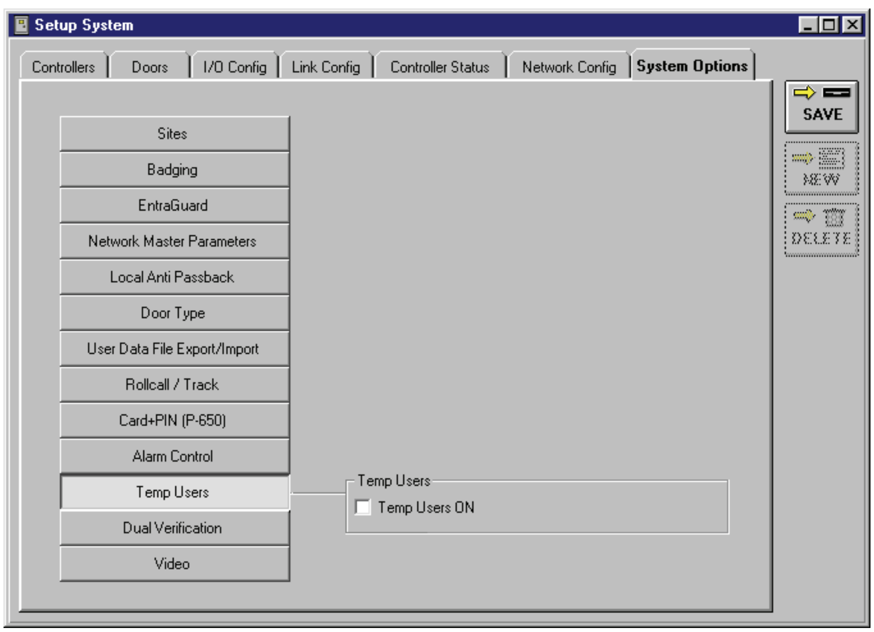


Figure 2-30: Temp Users Field

2. If your application does not use Temp Users, verify there is **not** a check mark in the Temp Users ON box. This is the default value (see Figure 2-30).
3. To enable temp users, click in the check box beside the Temp Users ON field. A check mark appears in the check box and the following window appears (see Figure 2-31 on page 27 of this section).

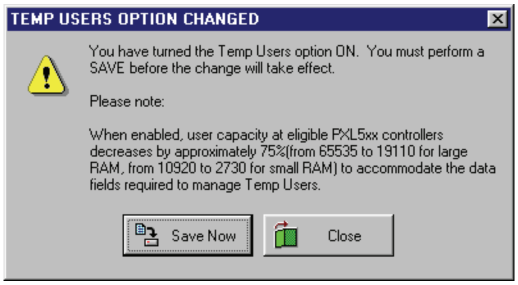


Figure 2-31: Temp Users Option Changed - ON

4. Click the 

button. A “Saved Configuration” window flashes on the screen.

5. Click on the 

button to save these changes. If the Temp Users changes are not saved before clicking any other button or exiting the System Options window, the data entered is lost and must be re-entered.

NOTE: A number of changes are made to the access control databases when the temp users feature is enabled. These changes add the fields necessary to set future activation and expiration dates. For simplicity in explaining the features in the Doors program, the majority of this Users Guide assumes that temp users mode is not enabled. The Temp Users feature is explained in “Temp Users” on page 1 in section 13.

1.2.17 Disable Temp Users

1. To disable the Temp Users feature, click in the Temp Users ON check box. The check mark that was there disappears and the following window appears (see Figure 2-32).

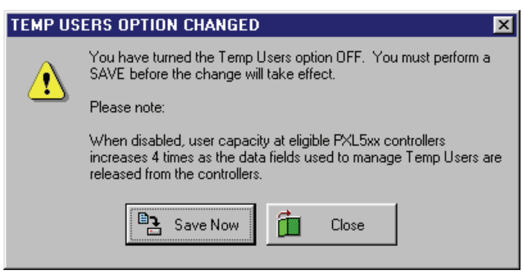
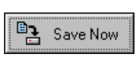


Figure 2-32: Temp Users Option Changed - OFF

2. Click the 

button. A “Saved Configuration” window flashes on the screen.

3. Click on the 

button to save these changes. If the Temp Users changes are not saved before clicking any other button or exiting the System Options window, the data entered is lost and must be re-entered.

1.2.18 Set Dual Verification

See "Dual Verification" on page 1 in section 14 for a complete description of how to enable, use, and disable the Dual Verification feature in *Doors*.

The Dual Verification parameter allows an operator to enable the dual verification feature of the *Doors* program.

NOTE: Dual Verification is for use with a PXL-500W/PXL-510W only.

The program default is for Dual Verification to be OFF.

1. From the System Options tab, click on the 

button. The System Options window will reveal the Dual Verification field (see Figure 2-33).

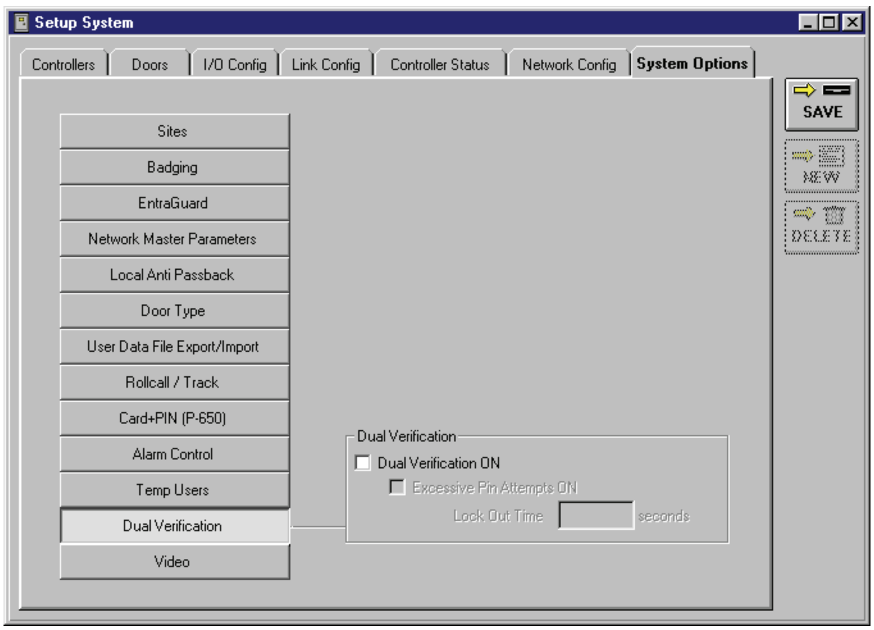


Figure 2-33: Dual Verification Field

2. If your system is not using Dual Verification, verify there is **not** a check mark in the Dual Verification ON box (see Figure 2-33).
3. To enable use of the Dual Verification feature, click in the check box beside the Dual Verification ON field. When there is a check in the box, the feature is enabled. To disable this field, click in the check box again and remove the check mark (this is the default value).

NOTE: A few changes are made to the access control databases when the Dual Verification feature is enabled. These changes add the fields necessary to manage dual verification. For simplicity in explaining the features in the Doors program, the majority of this Users Guide assumes that the Dual Verification feature is not enabled. Dual Verification related features are explained in detail in "Dual Verification" on page 1 in section 14.

1.2.19 Set Video

See "Visions Digital Video System" on page 1 in section 15 for a complete description of how to enable, use, and disable the Video feature in *Doors*.

The *Doors* Video feature allows for the integration of the *Visions* Digital Video System and *Doors*. Perform the following steps to enable the feature:

The program default is for Video to be OFF.

1. From the System Options tab, click on the 

button. The System Options window will reveal the Video field (see Figure 2-34).

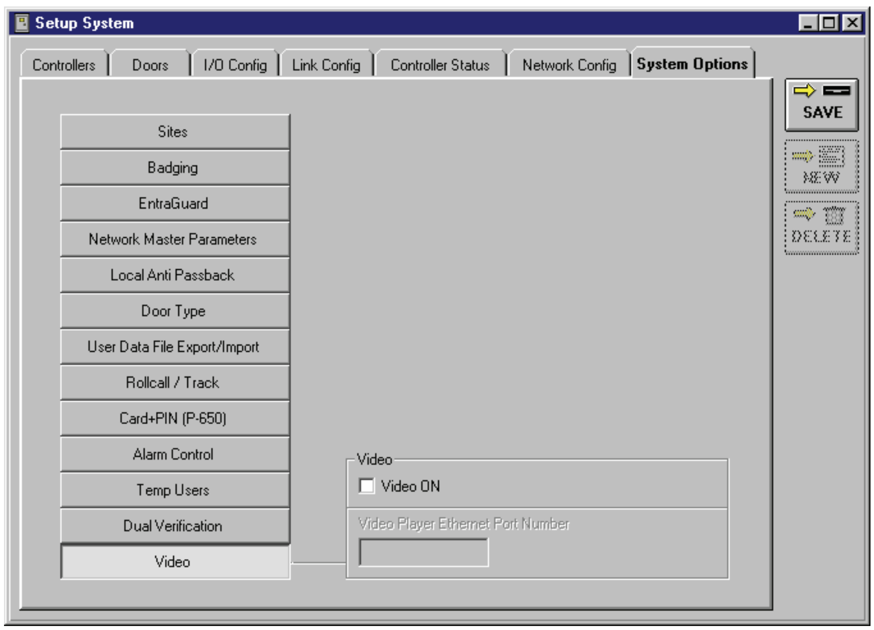


Figure 2-34: Video Field

2. To enable use of the Video feature, click on the **Video ON** check box. When there is a check in the box, the feature is enabled. To disable this field, click in the check box again and remove the check mark (this is the default value).

NOTE: A few changes are made to the access control databases when the Video feature is enabled. These changes add the fields necessary for Doors to communicate with the Visions Server. For simplicity in explaining the features in the Doors program, the majority of this Users Guide assumes that the Video feature is not enabled. Video related features are explained in detail in "Visions Digital Video System" on page 1 in section 15.

1.2.20 Disable Video

1. To disable Video, click in the **Video ON** check box. The check mark that was there disappears and the following window appears (see Figure 2-35).

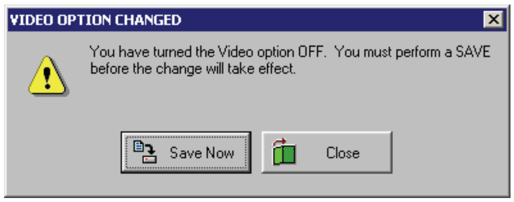


Figure 2-35: Video Option Changed - OFF

2. Click the  button. A “Saved Configuration” window flashes on the screen.

3. Click on the  button to save these changes. If the Video changes are not saved before clicking any other button or exiting the System Options window, the data entered is lost and must be re-entered.

4. Now click on the  button on the tool bar and update the access control network with the new information.

1.3 Save the System Parameters

1. When all information is entered/verified, click on the button and the new configuration information is saved to a configuration file. If the new system parameters are not saved before clicking any other button or exiting the setup system parameters window, the data entered is lost and must be re-entered.
2. The new system parameters should take effect immediately. If they do not, then the *Doors* program must be exited and restarted. To exit the *Doors* program, click on the File ⇒ Exit pull-down menu option or click in the box in the upper-right corner of the *Doors* window.
3. If you have not saved the new configuration information, the Data Has Changed warning will appear (see Figure 2-36).

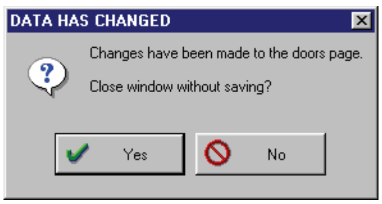


Figure 2-36: Data Has Changed Warning

4. If you want to close the window without saving the changes, click on the button. If you want to save the changes before closing, click on the button, then click on the button.
5. Exit the *Doors* program and start the *Doors* program per the instructions in “To Log On the Doors Program” on page 19 in section 1. The new system parameters now take effect and the program is ready to communicate with the access control network.

2.0 Autoconfiguration

The Autoconfiguration command is used to automatically retrieve controller/door configuration information from the access control network and insert that information into the appropriate controller/doors databases within the *Doors* program.

1. Click on the Setup ⇒ System pull-down menu or click on the button on the tool bar.
2. Click on the **Controllers** tab. The Setup System/Controllers window appears (see Figure 2-2 on page 3 of this section).
3. Ensure the access control network has been powered on per the instructions in the following documents:

PXL-250

- PXL-250 Start-Up Checklist (P/N 01852-001)
- PXL-250 Quick Start Guide (P/N 01835-002)
- PXL-250 Tiger Controller and SB-293 Satellite Board Technical Reference Manual (P/N 01836-004)

PXL-500

- PXL-500/PXL-510 Quick Start Guide (P/N 01918-001)

EntraGuard Gold

- EntraGuard Gold Quick Start Guide (P/N 01801-001)

4. Click on the button. The Net Communication window appears as communication is being established (see Figure 2-37).

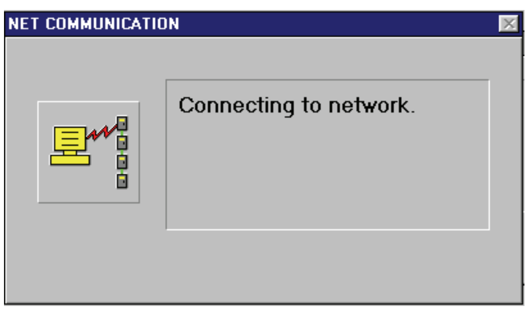


Figure 2-37: Connecting to the Network

5. Once communication has been established, the Autoconfiguration window appears indicating data is being transferred to the host computer (see Figure 2-38 on page 33 of this section).

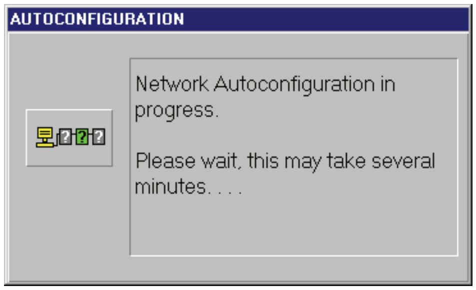


Figure 2-38: Autoconfiguration in Progress

2.1 Successful Autoconfiguration

1. The *Doors* software will automatically determine whether you have a satellite board connected to any of the controllers in the access network. For the controllers to which you do not have a satellite board connected, you will be prompted to select whether you want to name and configure a second reader for each controller (see Figure 2-39).

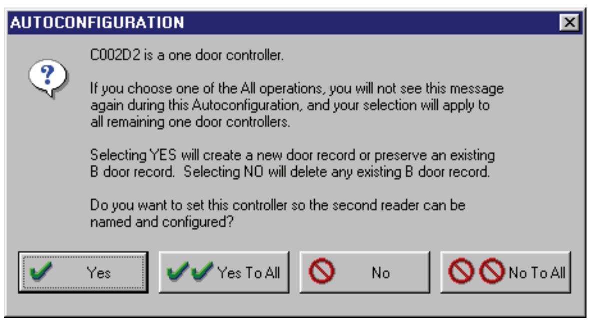
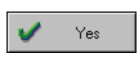
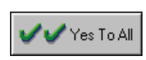


Figure 2-39: Setup of Multiple Readers

2. If you have connected two readers to this controller and you want to name and configure the second reader, click on the  button. If you have a large number of controllers and you want to name and configure a second reader on all of them, click on the  button.
3. If you have connected only one reader to this controller, or do not want to name and configure the second reader, click on the  button. If you have a large number of controllers and you do not want to name and configure a second reader on any of them, click on the  button.
4. When all data is received by the host computer, the Setup System/Controllers window displays the configuration information for all responding controllers on the access control network (see Figure 2-40 on page 34 of this section).

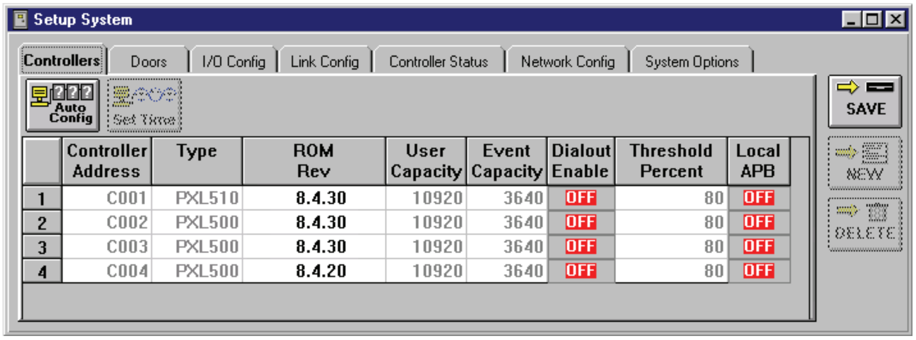


Figure 2-40: Successful Autoconfiguration Results

2.2 Failed Autoconfiguration

1. If the host computer cannot establish communication with the access control network, the Network Error window appears (see Figure 2-41).

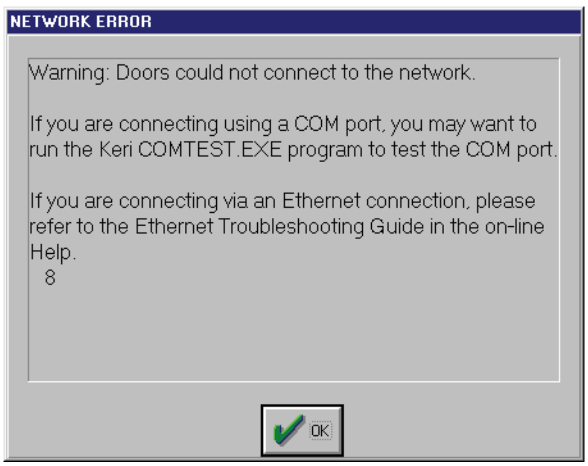


Figure 2-41: Unsuccessful Autoconfiguration

2. Click on the  button and the Autoconfiguration Error window appears (see Figure 2-42). If the  button is not selected within the time allotted, the window will automatically change to the Autoconfiguration Error window.

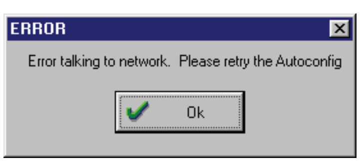


Figure 2-42: Autoconfiguration Error

3. Click on the  button.
4. Verify the following items.

For COM Port Operation

- the network parameters in the **Network Configuration** tab are correct: the COM port and the modem parameters (if applicable)
- the communication connections are fully operational (serial COM port, cabling, and modem as applicable)

For TCP/IP Operation

- the network parameters in the **Network Configuration** tab are correct: the TCP/IP port
- the network connections are fully operational (network card and cabling)

If the previous suggestions do not resolve the problem, please refer to either the PXL-250 Troubleshooting and Diagnostics Reference Document (P/N 01841-001) or the PXL-500/PXL-510 Troubleshooting and Diagnostics Reference Document (P/N 01917-001) to verify controller and cabling operations. If there is an EntraGuard controller on the network, refer to the EntraGuard Gold Troubleshooting and Diagnostics reference document (P/N 01912-001).

3.0 Set Controller Date and Time

The set time and date command is used to synchronize the time and date between the host computer and all the controllers on the access control network. Before synchronizing the host computer and the controllers, look at the date and time listed at the bottom of the *Doors* window. This is the date and time provided by the host computer. Be sure these values are correct. If they are not correct, change them per the instructions given in “Set the Host Computer Date and Time” on page 10 in section 1. If they are correct, perform the following steps.

1. Click on the Setup ⇒ System pull-down menu or click on the  icon on the tool bar. The Setup/ System window appears.
2. Click on the **Controllers** tab. The Controllers window appears (see Figure 2-40 on page 34 of this section).
3. Click on the 

button. After a brief pause, the Set Network Date And Time window appears (see Figure 2-43).

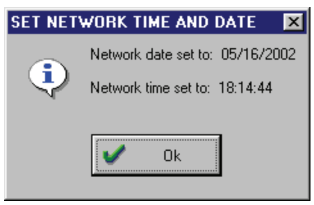
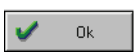


Figure 2-43: Setting Network Date and Time

4. The date and time kept by all controllers now matches that of the host computer. Click the 

button.

4.0 Network Update

The *Doors* software needs to download operating parameters to all controllers on the access control network. The Smart Update command uploads from the host computer to the access control network only the changes made to the *Doors* databases since the last update was performed. (For additional information see “Update and Collect Events from the Controllers” on page 35 in section 5.)

1. Click on the 

icon on the tool bar. The Update Network window appears. If changes have been made to the databases and the network needs to be updated, the Update Required field indicates this with a “Yes”, and the Skip/Update toggle box under the Smart Update Network field indicates “Update” (see Figure 2-44).

NOTE: When updating a new network for the first time or adding a new controller to an existing network, a Total Update must be performed on the system. Click on the “Skip” cell in the Total Update Network column to change the Skip” to a “Yes” then follow the rest of the instructions listed here.

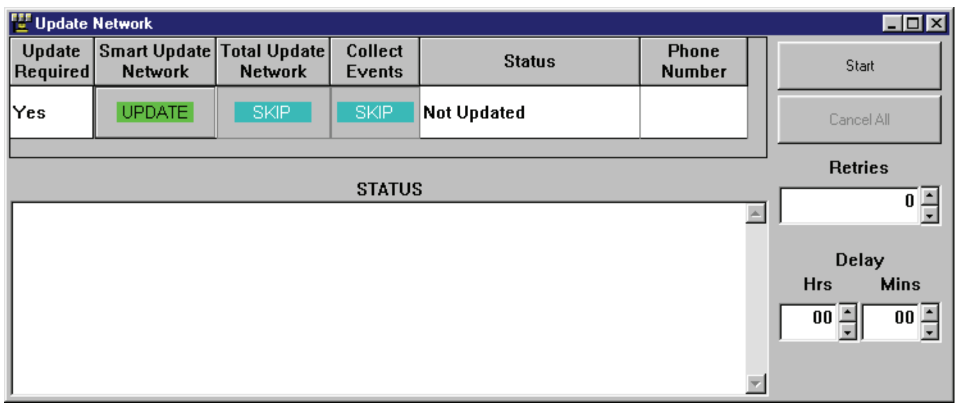


Figure 2-44: Required Network Update

2. Click on the 

button to begin Smart Update of the Network.

NOTE: Click on the ***Cancel All*** *button at any time to stop the update process.*

3. Once all parameters are collected, the host computer connects to the access control network (if it isn’t already connected). The Net Communication window appears if the access control network connection needs to be made (see Figure 2-45).

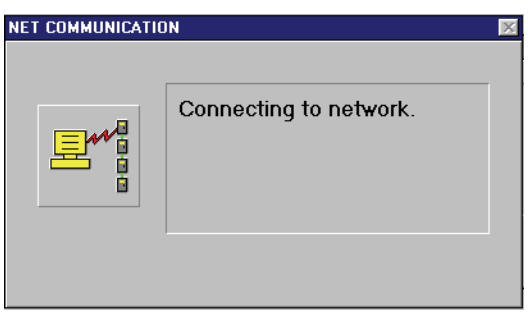


Figure 2-45: Connecting to the Network

4. Once the connection is made, the progress of the update may be viewed through the Status windows. The Status windows will indicate when the update is complete (see Figure 2-46 on page 38 of this section).

NOTE: Once the update process has begun, please be patient. The update process can take anywhere from several seconds to several minutes depending upon the amount of information to be updated and the number of controllers receiving information.

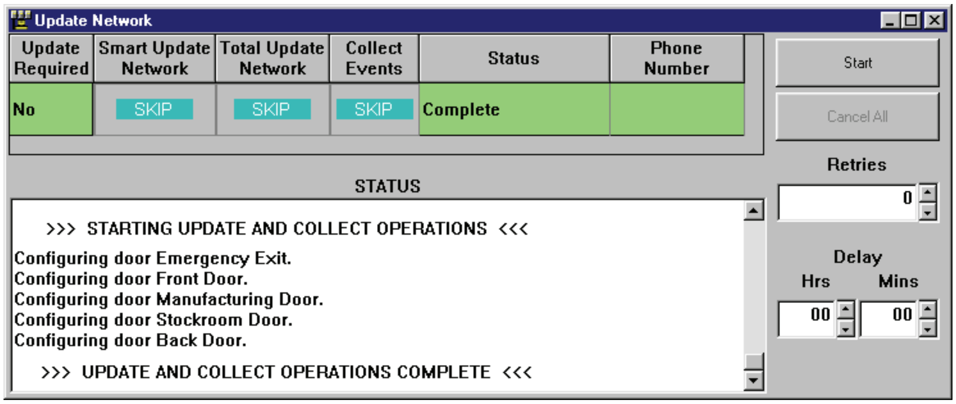


Figure 2-46: Successful Network Update

5. The access control network has now received all new default operating parameters and is ready for basic operation.

5.0 Get Controller Status

The **Controller Status** tab allows an operator to verify that all controllers/doors are recognized and to verify that the configuration information reported by the controller is correct.

5.1 Controller Status Fields

The following list shows the fields contained in the controller status spreadsheet with a short description of the information it gives.

Door Name
A descriptive text name for the door (this field should be blank for a new installation as the door name is assigned later in the database programming process – see "Assign a Door Name" on page 26 in section 3).

Address
The address of each controller recognized by the network and each door recognized by the controllers. There should be a line item in the spreadsheet for every controller/door in the access control network. The addresses listed should match the addresses programmed into each controller on the access control network.

Online
Indicates if the controller is ONLINE (the host computer **is** able to communicate with the controller) or OFFLINE (the host computer **is not** able to communicate with the controller).

Cltr Type
- If the field displays a PXL-250, this indicates the controller is a PXL-250 without a satellite board, and is capable of single-door control.
- If the field displays a PXL-500, this indicates the controller is a PXL-500 without a satellite board, and is capable of single-door control.
- If the field displays a PXL-510, this indicates the controller is a PXL-510 without a satellite board, and is capable of single-door control and alarm control.
- If the field displays an SB-293D, this indicates the controller is a PXL-250 with a satellite board that is configured to support two-door control, and has 6 inputs and 2 outputs.
- If the field displays an SB-593D, this indicates the controller is a PXL-500 or PXL-510 with a satellite board that is configured to support two-door control, and has 6 inputs and 2 outputs.
- If the field displays an SB-293X, this indicates the controller is a PXL-250 with a satellite board that is configured to support 8 inputs and 4 outputs (and does not control a second door).
- If the field displays an SB-593X, this indicates the controller is a PXL-500 or a PXL-510 with a satellite board that is configured to support 8 inputs and 4 outputs (and does not control a second door).
- If the field displays an EGGoldV, this indicates the controller is an EntraGuard Gold and is capable of single-door telephone entry control.

NOTE: When the letter S appears as the end of the display for a PXL-250 (i.e. PXL-250S), it refers to a surface mount controller.

ROM Rev
Displays the revision of the firmware EPROM on the controller.

RAM Config
Displays the size of the RAM on the PXL controller. The size of the RAM directly controls the number of cards that can be programmed into the PXL controller. PXL-250 with small RAM can manage up to 10,920 cards; Large RAM can manage up to 65,535 cards.

NOTE: The PXL-500 controller only comes in the large RAM format. However, if the Temp Users option is in use, the number of cards that can be programmed into the PXL-500/PXL-510 controller drops from 65,535 to 19,110.

Events
Displays the number of events currently stored in the controller. The maximum number of events that can be stored is 3,640.

Users In Memory
Displays the number of users enrolled into the controller (this field should be blank for a new installation as the user enrollment process is done later in the database programming process – see “Setup Users” on page 1 in section 4).

Date
Displays the date noted by the controller when controller status was requested.

Time
Displays the time noted by the controller when controller status was requested.
The remaining fields in the Controller Status spreadsheet are not valid until the access control database has been completely configured and downloaded to the controllers. The remaining fields relate to either the performance of the controller over time or to controller/door programming information that is done later in the database programming process. At this time, these fields all have initial or default values.

Cold Resets
Identifies how many cold resets have occurred on the controller. A cold reset indicates the controller's power has been cycled off and then on.

Warm Resets
Identifies how many warm resets have occurred on the controller. A warm reset occurs whenever the controller’s microprocessor gets “lost” during an operation, causing the microprocessor’s watchdog timer to reset the microprocessor. Reoccurring warm resets are indicative of a deteriorating controller or controller operating environment.

POST Fail
Identifies how many Power On Self Test (POST) failures have occurred on the controller. A POST failure indicates that either the controller’s RAM test failed during power up or the power supplied to the controller was too high or too low for proper operation.

Local APB
Identifies if local APB rules should be applied to this controller. Refer to “Set Local Anti Passback” on page 13 in this section.

Access Enabled
Identifies if the controller is enabled (allowed to grant access through reading cards/tags or entering a User ID) or disabled (ignores cards/tags and User IDs).

Reader Type (Controller)
Identifies the type of reader connected to the controller: Proximity, Wiegand, or None.

Door Status
Identifies the status of the door (i.e. open, closed, alarm, held open, forced) at the time controller status was read.

Door Lock
Identifies the status of the door lock (i.e. locked, unlocked, auto unlocked, time locked/unlocked) at the time controller status was read.

Door Unlock Time
Identifies the number of seconds a door will be unlocked following a valid access request.

Door Open Time
Identifies the number of seconds a door can be held open before a Door Held Open alarm is generated.

Auto Unlock/Lock Timezone
Identifies the unlock/lock timezone that has been assigned to the door. See “Set an Unlock/Lock Time Zone” on page 35 in section 3.

Auto Unlock/Lock Status
Identifies the current status of any unlock/lock timezone that has been assigned to the door (Active or Suspended). A dash in this column means the status was unknown. Check the controller type and prom version.

First Person In
Identifies the First Person In value that has been assigned to the door. See “First Person In” on page 36 in section 3.

Door Forced Output
Identifies which output relay will be triggered by a Door Forced event.

Door Held Output
Identifies which output relay will be triggered by a Door Held Open event.

Primary RTE
Identifies how the controller should respond to a primary Request to Exit input signal.

Aux RTE
Identifies how the controller should respond to an auxiliary Request to Exit input signal.

5.2 Get Status For All Controllers

1. Click on the Setup ⇒ System pull-down menu or click on the  button on the tool bar.
2. Click on the **Controller Status** tab. The Controller Status window appears (see Figure 2-47).

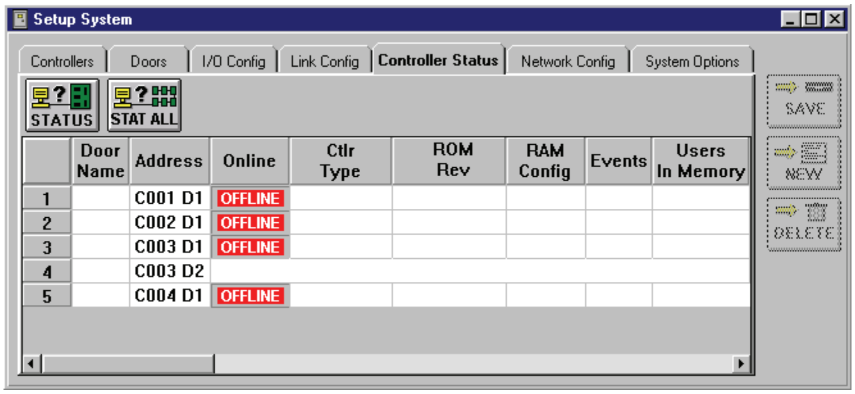


Figure 2-47: Controller Status Window

3. Click on the  button. All controllers are polled for their configuration and status, and this information is entered into the Controller Status spreadsheet (see Figure 2-48).

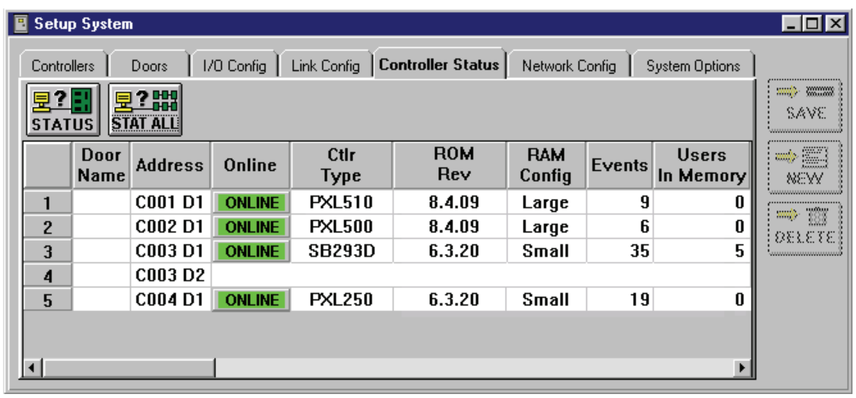


Figure 2-48: Received All Controllers’ Status

4. Each line of this spreadsheet corresponds to a controller/door. Verify the information displayed in the spreadsheet matches the configuration of the installed controllers. The following list describes the fields in the spreadsheet that should be verified at this time.

NOTE: Status information is at the moment of connection between the host computer and the access control network. The information is not updated and will remain the same until the next status request.

5.3 Get Status For One Controller

If work has been performed on one controller in the access control network (such as replacing or resetting the controller, changing the firmware, or changing the controller's configuration), that one controller can be polled for its status. Polling one controller saves time by not polling the status of the other controllers in the access control network.

1. Click on the Setup ⇒ System pull-down menu or click on the  button on the tool bar.
2. Click on the **Controller Status** tab. The Controller Status window appears (see Figure 2-49).

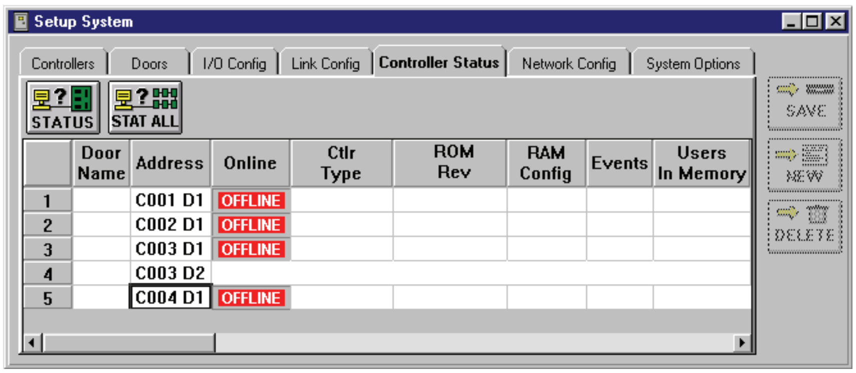


Figure 2-49: Selecting a Controller

3. Scroll up and down the list of controllers and locate the controller for which status is needed. Click in the **Address** cell for that controller (see Figure 2-49).
4. Click on the  button. The selected controller is polled for its configuration and status, and this information is entered into the Controller Status spreadsheet (see Figure 2-50).

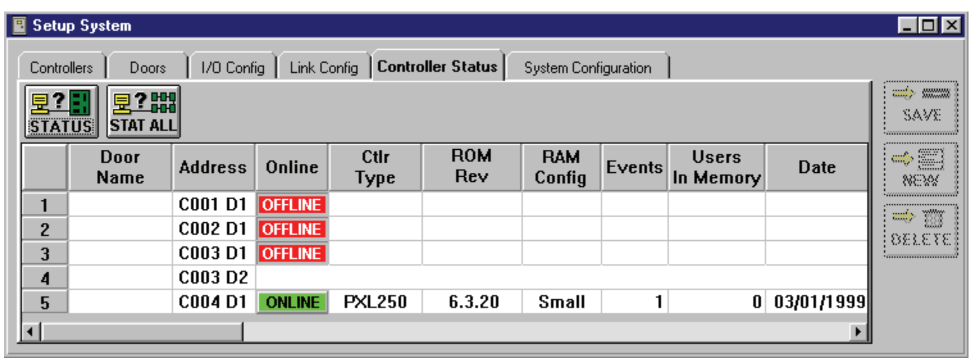


Figure 2-50: Received One Controller's Status

5. Verify the information displayed in the spreadsheet matches the configuration of the controller. Refer to "Controller Status Fields" on page 39 in this section for explanations of the fields in the controller status spreadsheet.

6.0 Set the Spreadsheet Font

To be able to print spreadsheet data from many ink-jet printers, the spreadsheet font must be set. This sets the font, font size, and font style displayed and printed by all spreadsheet windows.

NOTE: The System font is set as the Windows default font. However, for some printers, the System font automatically prints at 4 point size making a spreadsheet printout difficult to read. For ease of printing and screen formatting, Keri Systems recommends setting the spreadsheet font to a commonly used True Type font (such as Arial, Helvetica, or Times New Roman) at a commonly printed size (such as 11 or 12). The use of unique script fonts or large font sizes makes it difficult to format the spreadsheet's columns for viewing and printing.

1. Ensure all spreadsheets are closed.
2. Click the Setup ⇒ Spreadsheet Font pull-down menu option. The following window appears.

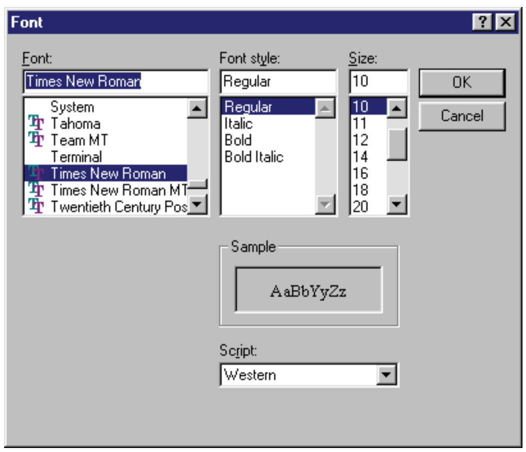
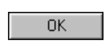
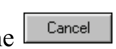


Figure 2-51: Spreadsheet Font Window

3. Scroll through the list of available fonts and click on the desired font.
4. Scroll through the list of available font styles and click on the desired style.
5. Scroll through the list of available font sizes and click on the desired size.
6. A sample of the selected font is displayed in the Sample field in the font window.
7. If the selected font is acceptable, click the  button.
8. To exit the spreadsheet font window without changing the current font, click on the  button.

NOTE: Although the File ⇒ Setup Printer pull-down menu command allows you to select a printer to which to print, due to a problem with the spreadsheet program, all spreadsheet data is printed to the default printer selected in the Windows Operating System Control Panel ⇒ Printer applet.

7.0 Setup Operators

This section describes the process for creating system operators and assigning operator privileges. The operators are the people who will be performing the work – creating the databases required by the *Doors* software to do its job and monitoring the system once everything has been downloaded to the controllers. Every operation performed by an operator has an operator identification number attached to it. This allows you to track operator performed changes.

Since the default operator has access rights to every operation, anyone who knows the default operator name and password will have complete programming access. Keri Systems recommends, at a minimum, changing the default operator name and password to protect your access control network.

7.1 Editing the Default Operator

1. Click on the Setup ⇒ Operators pull-down menu. The Setup Operators window appears (see Figure 2-52).

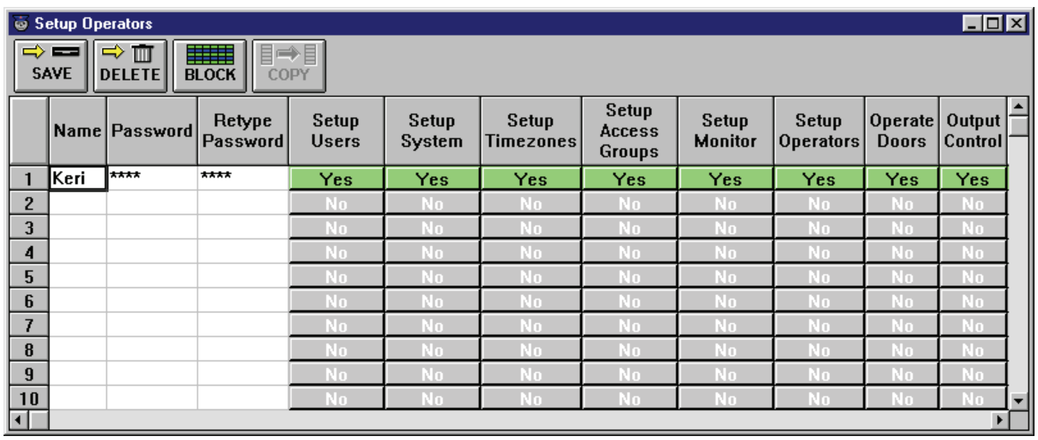


Figure 2-52: Setup Operators Window

NOTE: The Grant Amnesty operator option does not appear unless local anti passback is enabled (see "Set Local Anti Passback" on page 13 in this section).

2. Double-click in the "Name" field. The current operator name is highlighted. Type a descriptive name for the operator being assigned Operator Number 1 (the default operator).

NOTE: There is a 15 character maximum for the operator name.

3. It is essential that the default operator has the ability to perform any and every action within the *Doors* program. Verify every option is set to Yes so that Operator Number 1 will have full access to all program options. Use the scroll on the bottom to view all the operator options.
4. Double-click in the "Password" field. For the Password, enter a string of characters or numbers, 4 characters minimum to 8 characters maximum, case sensitive (that is, the program does keep track of UPPERCASE versus lowercase characters). The password should be something easily remembered by the operator, but not easily guessed by unauthorized personnel.
5. To ensure that the password entered is correct, it must be entered again in the "Retype Password" field. The characters entered into the "Retype Password" field must exactly match the Password field.

6. Click on the 

button to save these changes. If the operator changes are not saved before clicking any other button or exiting the setup operators window, the data entered is lost and must be re-entered.
7. If the “Password” and “Retype Password” fields do not match exactly, the password is rejected and the Password Error warning appears (see Figure 2-53).



Figure 2-53: Password Error Warning

8. Click on the 

button to return to the Setup Operators window.
9. Double-click in the “Retype Password” field and enter the password. If the Password Error window appears again, return to the Setup Operators window and enter both passwords again.
10. Click on the 

button to save these changes. If the operator changes are not saved before clicking any other button or exiting the setup operators window, the data entered is lost and must be re-entered.

7.2 Creating a New Operator

Depending upon the assignment choice, each Operator assignment is set to one of these three values.

NO
The operator does not have operation rights.

YES
The operator does have operation rights.

Read Only
The operator can view, but not make any changes to this operation.

Do a little planning before assigning operator operation rights.

- determine how many operators are needed to cover operation of the access control system
- consider any time of day and day of the week requirements
- determine the requirements and responsibilities of these operators
- use the following list and determine which operators should have what responsibilities

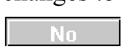
1. From the Setup Operators window (see Figure 2-52 on page 45 of this section), click in the next operator slot that is unassigned (there are 32 operator slots).
2. Click in the name cell and assign an operator name.
3. Click in the password cell and enter the operator's password.
4. Click in the retype password cell and retype the operator's password.

NOTE: The operator name, password, and retype password fields are all case sensitive. That is, the program differentiates between UPPERCASE and lowercase in all three fields. Please keep this in mind when creating operator names and passwords.

5. For each operator option on the screen, click on the 

cell that corresponds to the operator responsibilities being granted. The cell changes to 

. Click on the cell again and it changes to 

. Click on the cell one more time and it returns to the original position of 

. (For a complete list of operator responsibilities that must be granted, see "Operator Rights" on page 48.)
6. Once all rights have been assigned, click on the 

button to save these changes. If the operator changes are not saved before clicking any other button or exiting the setup operators window, the data entered is lost and must be re-entered.

7.2.1 Operator Rights

The following list are the feature operation rights available for assignment to an operator (refer to Figure 2-52 on page 45 of this section). Each operator must be created and saved, one-at-a-time. There is a limit of 32 operators that can be assigned. Repeat this process for each operator to be assigned.

Setup Users
Identifies if an operator is allowed to perform the Setup Users commands: enrolling users, entering data, voiding, deleting, and assigning access groups, or is allowed to have Read Only access to review, but not change, this information. If Read Only access is selected, the operator will not be allowed to view Card+PIN information.

Setup System
Identifies if an operator is allowed to perform the Setup System commands: entering or editing the parameters by which a door/controller operates, or is allowed to have Read Only access to review, but not change, this information.

Setup Timezones
Identifies if an operator is allowed to perform the Setup Timezone commands: creating or editing Timezones and Holiday schedules, or is allowed to have Read Only access to review, but not change, this information.

Setup Access Groups
Identifies if an operator is allowed to perform the Setup Access Group commands: creating or editing access groups (specifically associating timezones with doors), or is allowed to have Read Only access to review, but not change, this information.

Setup Monitor
Identifies if an operator is allowed to modify a Monitor window (a window that views events on the access control network as they happen), or is allowed to have Read Only access to review, but not change, this information.

Setup Operators
Identifies if an operator is allowed to create new operators.

Setup Video
Identifies if an operator is allowed to enable the video feature.

Operate Doors
Identifies if an operator is allowed to manually lock and unlock doors using program commands and to perform complete database updates of selected controllers on the access control network.

Output Control
Identifies if an operator is allowed to manually operate output relays (turn them on and off).

Grant Amnesty
Identifies if an operator is allowed to manually grant anti passback amnesty to cardholders.

Start Monitor
Identifies if an operator is allowed to start the event monitoring process.

Stop Monitor
Identifies if an operator is allowed to stop the event monitoring process.

Start Monitor #1, #2, #3
Identifies which of the three definable event monitors an operator may open.

Event Reports
Identifies if an operator is allowed to generate Searchable Event reports (summaries of events that have occurred on the access control network).

Doors Reports
Identifies if an operator is allowed to generate Formatted reports (pre-programmed reports of controller events and system parameters).

Launch Backup
Identifies if an operator is allowed to generate Formatted reports (pre-programmed reports of controller events and system parameters).

Exit Program
Identifies if an operator is allowed to exit the *Doors* program, returning to the operating system.

NOTE: Exiting the program does not end the access control process. Once all information is entered and uploaded to all controllers, the controllers manage access by themselves and the Doors program is only needed for uploading changes to the controllers or for downloading event information from the controllers, generating event reports, and for real-time event monitoring.

Enroll
Identifies if an operator is allowed to enroll new users.

Show Secondary ID
Identifies if an operator is allowed to

End of section.

Section 3

Database Programming

The database programming section describes the process for entering the day to day operating parameters for the access control network. This section describes the following eight operations.

- Setup Time Zones – defining daily and holiday access time periods to be applied to doors
- Configure Dedicated I/O Points – configuring input and output points to be used by auxiliary RTE, door forced alarms, and door held open alarms
- Setup Controllers/Doors – configuring controller/door operation on the access control network
- Setup Access Groups – defining access groups: supersets of time zone and door information to which users are assigned

Document Number 01914-003, Revision 5.4 – May, 2004

1.0 Setup Time Zones

The setup time zones section describes the process for defining the daily and holiday access time periods to be applied to doors in access groups and applied to automatic door locking/unlocking control. A time zone is defined as the hours-of-the-day when a user is granted access to a secure area.

Up to 32 time zones can be defined. Four separate start/stop periods can be programmed for each day-of-the-week and for up to three holiday schedules. This provides an incredible amount of flexibility in setting time zone work schedules for the users using the access control system.

This section provides examples of time zones for a day-shift employee, a janitorial employee, a grave-shift employee, and one holiday schedule. Before defining time zones, take some time and map out all the time zone usage possibilities for the site. Consider the variety of access hours for employees and customers, and consider special requirements such as janitorial personnel (may require night access), service/repair personnel (may require all hours access), supervisory/management staff (may require extended hours access), and shift personnel (first/day, second/swing, third/grave, flex).

NOTE: All time values used and stored by the Doors program are in 24-hour format. For example: midnight is stored as 00:00 hours, 8 A.M. is stored as 08:00 hours, noon is stored as 12:00 hours, 6 P.M. is stored as 18:00 hours, and 11:30 P.M. is stored as 23:30 hours.

NOTE: The use of descriptive names when naming time zones and access groups can make the report viewing process easier, but please avoid the tendency to assign similar names to time zones and access groups. It can be helpful to use TZ and AG as a prefix or suffix when assigning names to make the distinction between time zone and access group easier. Or, it can be helpful to assign to the time zone a name that reflects the days-of-the-week and the time-of-day access should be granted, and assign to the access group a name that describes the users that will be assigned to the access group.

1.1 Time Zone Window

1. To reach the Setup Timezones window, click on Setup ⇒ Timezones or click on the  icon on the tool bar. The Setup Timezones window appears (see Figure 3-1).

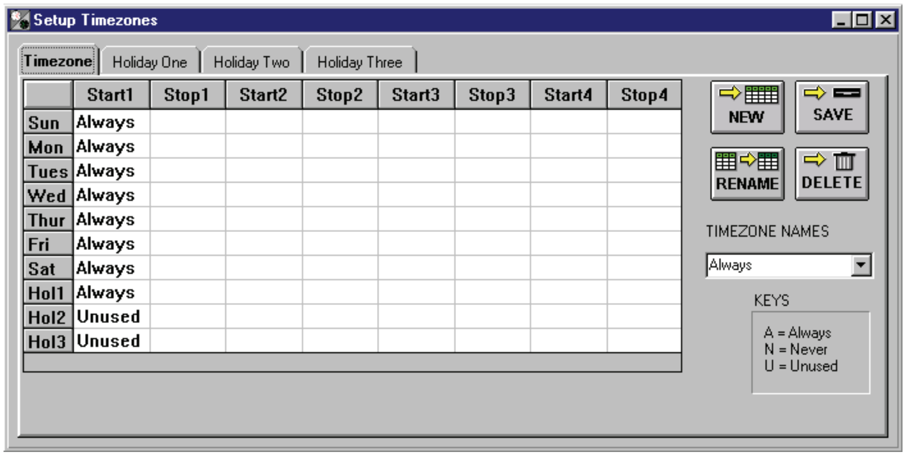


Figure 3-1: Setup Timezones Window

1.1.1 Time Zone Fields

Timezone Tab
Displays the day-of-the-week / hours-of-the-day spreadsheet window.

Holiday One, Two, Three Tabs
Displays the holiday date/holiday name spreadsheet windows.

New Button
Clears the spreadsheet in preparation for new data entry.

Save Button
Saves the spreadsheet information.

Rename Button
Renames the time zone named in the “Timezone Names” field.

Delete Button
Deletes the time zone named in the “Timezone Names” field, removing its information from the time zone database.

Keys Field
Identifies three defined cell values: Always, Never, and Unused. Click on a cell and type the first letter of the key word (A, N, U). An Always cell always **allows** access on that day-of-the-week. A Never cell **never** allows access on that day-of-the-week. An Unused cell (used on the holiday schedules only) indicates that a holiday schedule has not been applied.

There are two predefined time zones, available in the Timezone Names pull-down menu: Always and Never. These time zones are not editable. The Always time zone always allows access regardless of time-of-day or day-of-the-week. The Never time zone never allows access regardless of time-of-day or day-of-the-week.

1.2 Day-Shift Time Zone Example

This time zone example is designed for a day-shift employee, eligible to work an 8 hour shift at any time within the day-shift time zone.

1. Create a list of the days-of-the-week and the hours-of-the-day when an access group should allow access for this time zone. The following list describes this day-shift time zone.

- Monday through Friday – 06:00 to 20:00 hours (6 A.M. to 8 P.M.)
- Saturday – 08:00 to 18:00 hours (8 A.M. to 6 P.M.)
- Sunday – no access allowed
- Holidays – 08:00 to 12:00 hours (8 A.M. to Noon)

2. From the Setup Timezones window (see Figure 3-1 on page 4 of this section), click on the 

button. The day-of-the-week start fields and the Timezone Names field are cleared (see Figure 3-2).

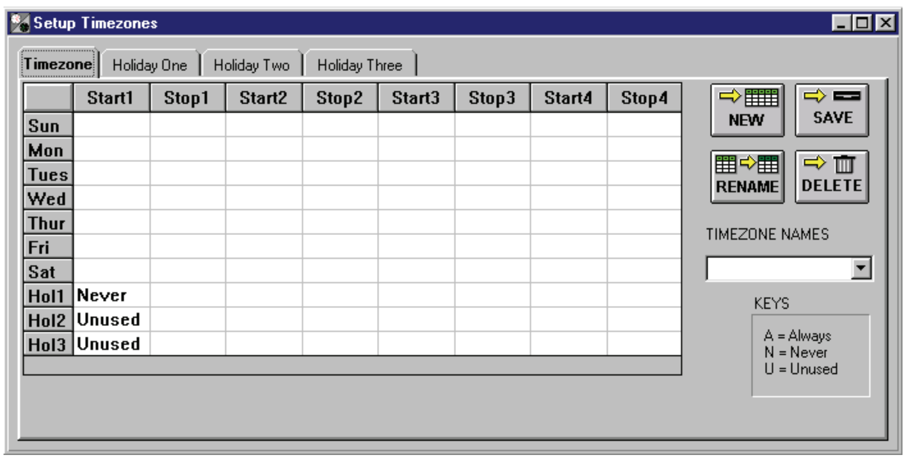


Figure 3-2: Cleared Setup Timezones Window

3. Following the day-shift parameters given in Step 1, no access is allowed on Sunday. Double-click in the Sunday Start1 cell and type **N**. The “Never” key appears in the cell setting this time segment to never allow access on Sunday.
4. Double-click in the Monday Start1 cell and type **06:00**. When you directly type in the cell, you must type in every number. The *Doors* software recognizes invalid times and will not allow you to type in a 6 without first typing in the leading 0.

*NOTE: When you double-click in a cell, a spinner icon appears (see Figure 3-3 on page 6 of this section). If you click on the hour side of the time (**00**:00), you can use the spinner to advance the hours forward or backward and select a desired hour. If you click on the minute side of the time (00:**00**), you can use the spinner to advance the minutes forward or backward and select a desired minute. You may decide to use this method to set the time instead of directly typing the information into a cell.*

5. Double-click in the Monday Stop1 cell and set the time to **20:00**.
6. Repeat steps 5 and 6 for the Tuesday through Friday Start 1 cells and Stop1 cells.
7. Double-click in the Saturday Start1 cell and set the time to **08:00**.
8. Double-click in the Saturday Stop1 cell and set the time to **18:00**.
9. Double-click in the Hol1 Start1 cell and set the time to **08:00**.
10. Double-click in the Hol1 Stop1 cell and set the time to **12:00**.

11. Click in the "Timezone Names" field and type **Day Shift TZ**. The Setup Timezones window should appear identical to Figure 3-3. Any discrepancies can be corrected by clicking on the cell or field and making the correction.

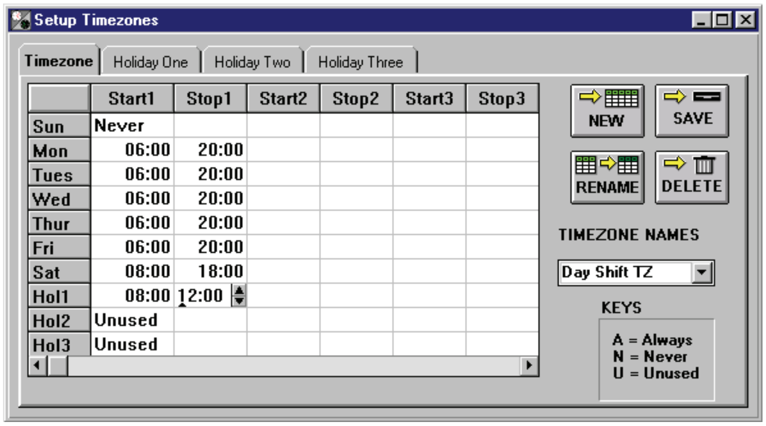


Figure 3-3: Day-Shift Time Zone Example

12. Once everything has been verified as correct per the time zone list, click on the  button. If the time zone is not saved before clicking any other button or exiting the Setup Timezones window, the data entered is lost and must be re-entered.

13. Now update the access control network with the new information. Click on the  button on the tool bar (for details on the update process refer to "Update the Network" on page 35 in section 5).

1.3 Janitorial Shift Time Zone Example

This time zone example is designed for a janitorial staff employee, eligible to work four hours a night, three times a week.

1. Create a list of the days-of-the-week and the hours-of-the-day that an access group should have access for this time zone. The following list describes this janitorial shift time zone.

- Sunday, Tuesday, and Thursday – 18:00 to 22:00 hours (6 P.M. to 10 P.M.)

2. From the Setup Timezones window (see Figure 3-1 on page 4 of this section), click on the 

button. The day-of-the-week start fields and the time zone name field are cleared (see Figure 3-2 on page 5 of this section).
3. Following the janitorial shift parameters given in Step 1, no access is allowed on Monday, Wednesday, Friday, and Saturday. Double-click in the Monday Start1 cell and type **N**. The "Never" key appears in the cell setting this time segment to never allow access on Monday. Repeat this step for the Wednesday, Friday, and Saturday Start1 cells.
4. Double-click in the Sunday Start1 cell and set the time to **18:00**.
5. Double-click in the Sunday Stop1 cell and set the time to **22:00**.
6. Repeat steps 5 and 6 for the Tuesday and Thursday Start 1 and Stop1 cells.
7. Click in the "Timezone Names" field and type **Janitorial Shift TZ**. The Setup Timezones window should appear identical to Figure 3-4. Any discrepancies can be corrected by clicking on the cell or field and making the correction.

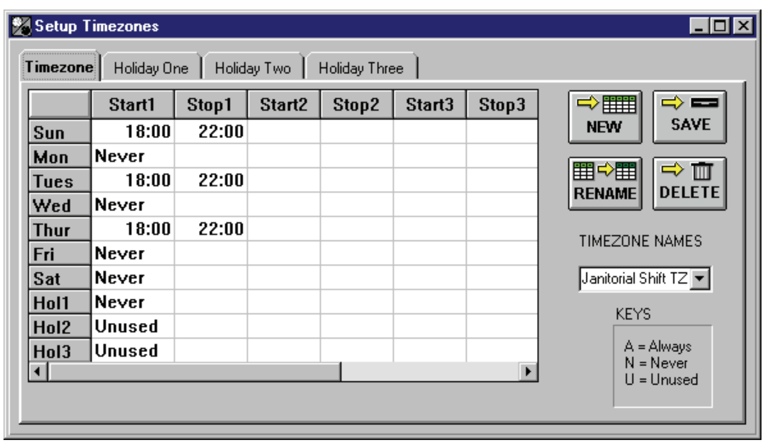
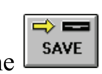


Figure 3-4: Janitorial Shift Time Zone Example

8. Once everything has been verified as correct per the time zone list, click on the 

button. If the time zone is not saved before clicking any other button or exiting the Setup Timezones window, the data entered is lost and must be re-entered.

9. Now update the access control network with the new information. Click on the 

button on the tool bar (for details on the update process refer to "Update the Network" on page 35 in section 5).

1.4 Graveyard Shift Time Zone Example (Crossing Midnight)

This time zone example is designed for a graveyard shift employee, eligible to work from 11:30 P.M. to 7:30 A.M. Monday/Tuesday through Friday/Saturday.

The graveyard shift time zone is unique in that it starts in one day-of-the-week and ends in the next day-of-the-week. To accommodate this, the time zone uses both the Start1/Stop1 and Start2/Stop2 cells to cover the split in access times Tuesday through Friday.

1. Create a list of the days-of-the-week and the hours-of-the-day that an access group should have access for this time zone. The following list describes this graveyard shift time zone.

- Monday – 11:30 to Tuesday – 07:30 hours (11:30 P.M. to 7:30 A.M.)
- Tuesday – 11:30 to Wednesday – 07:30 hours (11:30 P.M. to 7:30 A.M.)
- Wednesday – 11:30 to Thursday – 07:30 hours (11:30 P.M. to 7:30 A.M.)
- Thursday – 11:30 to Friday – 07:30 hours (11:30 P.M. to 7:30 A.M.)
- Friday – 11:30 to Saturday – 07:30 hours (11:30 P.M. to 7:30 A.M.)

2. From the Setup Timezones window (see Figure 3-1 on page 4 of this section), click on the 

button. The day-of-the-week start fields and the time zone name field are cleared (see Figure 3-2 on page 5 of this section).
3. Following the graveyard shift parameters given in Step 1 above, no access is allowed on Sunday. Double-click in the Sunday Start1 cell and type **N**. The “Never” key appears in the cell setting this time segment to never allow access on Sunday.
4. Double-click in the Monday Start1 cell and set the time to **23:30**. Double-click in the Monday Stop1 cell and set the time to **00:00**. Monday access is limited to the hours between 11:30 P.M. and Midnight.
5. Double-click in the Tuesday Start1 cell and set the time to **00:00**. Double-click in the Tuesday Stop1 cell and set the time to **07:30**. Double-click in the Tuesday Start2 cell and set the time to **23:30**. Double-click in the Tuesday Stop2 cell and set the time to **00:00**. Tuesday access is split between Midnight to 7:30 A.M. (to cover the end of the shift that began on Monday) and 11:30 P.M. to Midnight (to cover the beginning of the shift on Tuesday).
6. Repeat step 6 for Wednesday through Friday.
7. Double-click in the Saturday Start1 cell and set the time to **00:00**. Double-click in the Saturday Stop1 cell and set the time to **07:30**. Saturday access is limited to the hours between Midnight and 7:30 A.M.
8. Click in the “Timezone Names” field and type **Graveyard Shift TZ**. The Setup Timezones window should appear identical to Figure 3-5 on page 9 of this section. Any discrepancies can be corrected by clicking on the cell or field and making the correction.

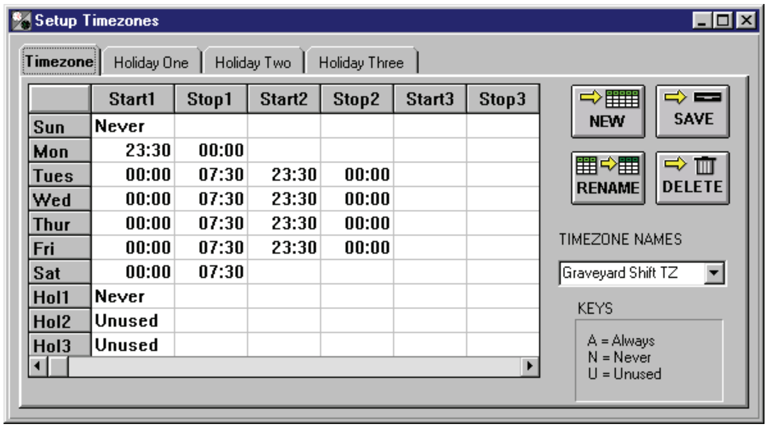


Figure 3-5: Graveyard Shift Time Zone Example

9. Once everything has been verified as correct per the time zone list, click on the 

button. If the time zone is not saved before clicking any other button or exiting the Setup Timezones window, the data entered is lost and must be re-entered.

10. Now update the access control network with the new information. Click on the 

button on the tool bar (for details on the update process refer to "Update the Network" on page 35 in section 5).

1.5 Display/Edit a Time Zone

The following instructions explain how to display and edit the contents of a time zone.

1. Click on Setup ⇒ Timezones or click on the icon on the tool bar. The Setup Timezones window appears (see Figure 3-1 on page 4 of this section).
2. Click on the arrow in the Timezone Names field. A list of all saved time zones is displayed.
3. Scroll through the list until the desired time zone is located.
4. Click on that time zone name and the time zone is displayed in the spreadsheet.
5. Review the data displayed. If any edits need to be made, click in the cell needing editing and type the new value for that cell.
6. Once edits have been made, click on the button. If the edits are not saved before clicking any other button or exiting the Setup Timezones window, the data entered is lost and must be re-entered.
7. Now update the access control network with the new information. Click on the button on the tool bar (for details on the update process refer to “Update the Network” on page 35 in section 5).

1.6 Rename a Time Zone

The following instructions explain how to rename a time zone.

1. Click on Setup ⇒ Timezones or click on the icon on the tool bar. The Setup Timezones window appears (see Figure 3-1 on page 4 of this section).
2. Click on the arrow in the Timezone Names field. A list of all saved time zones is displayed.
3. Scroll through the list until the desired time zone is located.
4. Click on that time zone name and the time zone is displayed in the spreadsheet.
5. Make sure the time zone name is highlighted then type in the new time zone name.
6. Click on the button. The new time zone name will automatically be updated throughout the *Doors* software.

NOTE: If you click on the button instead of the button, the time zone will not be renamed, but a new time zone will be added.

1.7 Delete a Time Zone

If a time zone becomes unneeded it can be deleted.

NOTE: Once deleted, a time zone is not recoverable. If a time zone was deleted by mistake, it must be recreated.

NOTE: If a time zone is in use by an access group in the access control network, the Doors program will not allow it to be deleted. Review all access groups to ensure all references to the time zone to be deleted have been changed.

1. Click on Setup ⇒ Timezones or click on the  icon on the tool bar. The Setup Timezones window appears (see Figure 3-1 on page 4 of this section).
2. Click on the  arrow in the Timezone Names field. A list of all saved time zones is displayed.
3. Scroll through the list until the desired time zone is located.
4. Click on that time zone name and the time zone is displayed in the spreadsheet.
5. Review the data displayed and verify this is the time zone to be deleted.
6. Click on the  button.
7. If the time zone is not in use anywhere in the *Doors* program, the time zone is deleted and the spreadsheet is cleared.
8. If the time zone is still in use somewhere in the *Doors* program, the Timezone In Use Error message appears (see Figure 3-6).

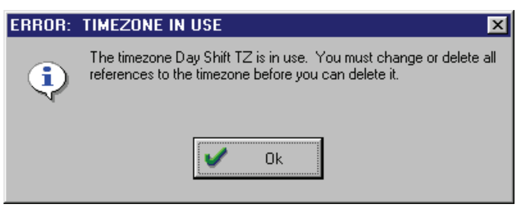
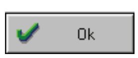


Figure 3-6: Timezone In Use Error Message

9. Click on the  button. Review all access groups and change where the time zone is used. Then repeat the steps for deletion as described above.
10. Once the deletion has been performed, click on the  button. If the deletion is not saved before clicking any other button or exiting the Setup Timezones window, the deletion does not take affect and the time zone remains in the system.
11. Now update the access control network with the new information. Click on the  button on the tool bar (for details on the update process refer to "Update the Network" on page 35 in section 5).

2.0 Holiday Schedules

Holidays are treated as if they are just another day of the week. This allows holidays to have access time periods applied to them. Three holiday schedules are available for definition. This allows certain holidays to have different access times than others do. For example, on holidays such as Presidents' Day or Martin Luther King's birthday government offices are closed but many businesses remain open; on holidays such as Christmas or Thanksgiving virtually all business and government offices are closed. An access control network might need to assign holiday access times differently to cover these two types of holidays.

Before defining holiday schedules, take some time and map out all the holiday possibilities for the site. Consider the relative importance of the holiday and determine if multiple holiday schedules are required.

NOTE: Certain holiday dates change from year-to-year (i.e. Easter or Thanksgiving). Operators should review and update the holiday schedules prior to the beginning of a new year to ensure proper holiday coverage.

2.1 Create a Holiday Schedule

1. Create a list of the holiday names and dates that should be applied to time zones. This list can crossover to the following year. The following is an example of a possible holiday schedule.

- 01/01/2001 – New Year's Day
- 02/19/2001 – Presidents' Day
- 05/28/2001 – Memorial Day
- 07/04/2001 – Independence Day
- 09/03/2001 – Labor Day
- 11/22/2001 – Thanksgiving Day
- 11/23/2001 – Day after Thanksgiving
- 12/24/2001 – Christmas Eve
- 12/25/2001 – Christmas Day
- 12/31/2001 – New Year's Eve
- 01/01/2002 – New Year's Day

2. Click on Setup ⇒ Timezones or click on the  icon on the tool bar. The Setup Timezones window appears (see Figure 3-1 on page 4 of this section).
3. Click on the **Holiday One** tab. The Holiday One window appears (see Figure 3-7 on page 13 of this section).

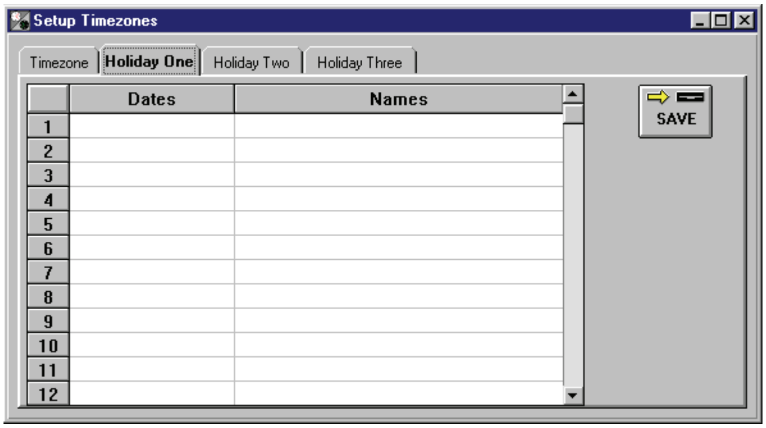


Figure 3-7: Holiday One Entry Window

4. Click on the Dates/1 cell and type **01/01/2001**.

*NOTE: When you double-click in a cell, a spinner icon appears (see Figure 3-8). If you click on the month side of the date (**00**/00/0000), you can use the spinner to advance the month forward or backward and select the desired month. If you click on the day side of the date (00/**00**/0000), you can use the spinner to advance the day forward or backward and select the desired day. If you click on the year side of the date (00/00/**0000**), you can use the spinner to advance the year forward or backward and select the desired year. You may decide to use this method to set the date instead of directly typing the information into the cell.*

NOTE: When you double-click in a cell with a spinner icon, a calendar appears with today's date (see Figure 3-8). Click on the left and right arrows on the month and year bars to display the desired month and year, then click on the desired day. You may decide to use this method to set the date instead of directly typing the information into the cell or using the spinner icon.

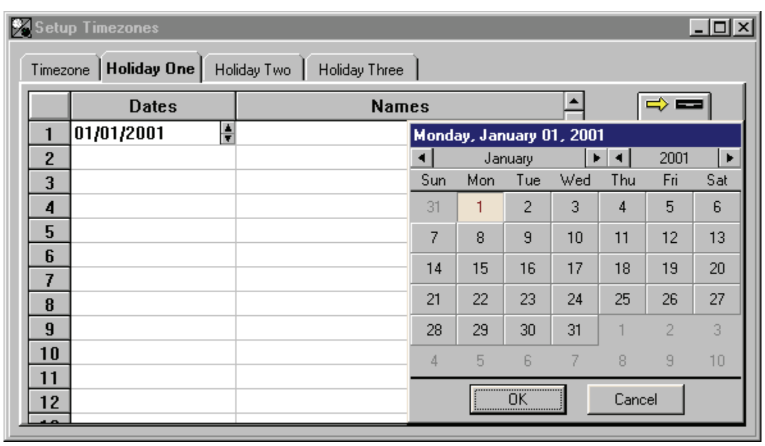


Figure 3-8: Holiday Date Entry by Spinner Icon or Calendar

5. Click on the Names/1 cell and type **New Year's Day**.
6. Working down through the spreadsheet, repeat step 4 for each holiday in the list in Step 1.
7. When complete, the holiday one schedule should appear similar to Figure 3-9 on page 14 of this section. Any discrepancies can be corrected by clicking on the cell or field and making the correction.

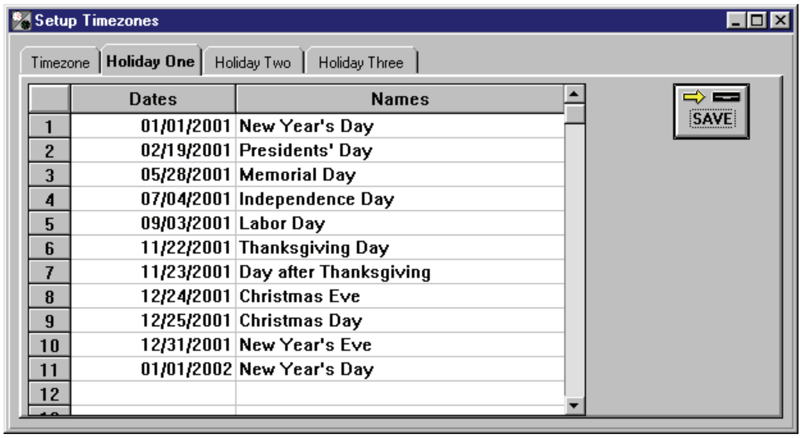


Figure 3-9: Holiday One Example Schedule

8. Once everything has been verified as correct per the holiday list, click on the  button. If the holiday schedule is not saved before clicking any other button or exiting the Setup Timezones window, the data entered is lost and must be re-entered.

9. Now update the access control network with the new information. Click on the  button on the tool bar (for details on the update process refer to "Update the Network" on page 35 in section 5).

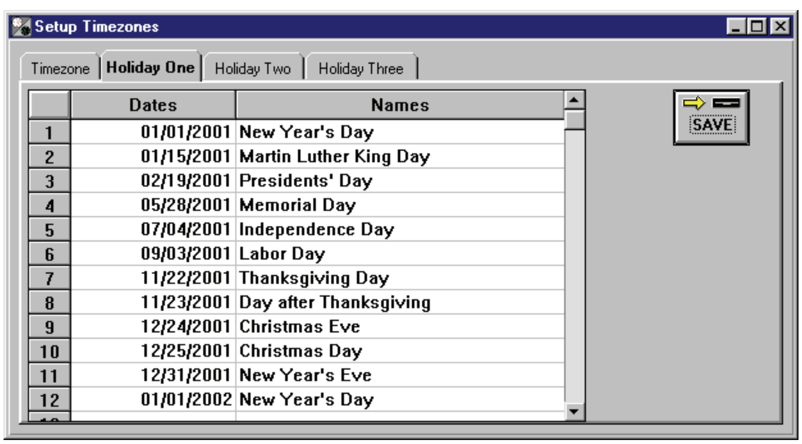
2.2 Display/Edit a Holiday Schedule

The following instructions explain how to display and edit the contents of a holiday schedule.

1. Click on Setup ⇒ Timezones or click on the  icon on the tool bar. The Setup Timezones window appears (see Figure 3-1 on page 4 of this section).
2. Click on the Holiday One tab. The holiday one schedule is displayed (see Figure 3-9 on page 14 of this section).
3. Review the data displayed. If any edits need to be made, simply click in the cell needing editing and type the new value for that cell.
4. Once all necessary changes have been made, click on the  button. If the holiday schedule is not saved before clicking any other button or exiting the Setup Timezones window, the data entered is lost and must be re-entered.

2.2.1 To Add a New Holiday

1. To add a new holiday scroll through the list of holidays and locate the first set of open Dates/Names cells. Enter the holiday date and name as described in “Holiday Schedules” on page 12 of this section. For example, Click on the open Dates cell and type **01/15/2001**. Click on the open Names cell and type **Martin Luther King Day**.
2. Click on the  button. If the holiday schedule is not saved before clicking any other button or exiting the Setup Timezones window, the data entered is lost and must be re-entered. Once the save is complete the holiday schedule is sorted and displayed in order (see Figure 3-10)



	Dates	Names
1	01/01/2001	New Year's Day
2	01/15/2001	Martin Luther King Day
3	02/19/2001	Presidents' Day
4	05/28/2001	Memorial Day
5	07/04/2001	Independence Day
6	09/03/2001	Labor Day
7	11/22/2001	Thanksgiving Day
8	11/23/2001	Day after Thanksgiving
9	12/24/2001	Christmas Eve
10	12/25/2001	Christmas Day
11	12/31/2001	New Year's Eve
12	01/01/2002	New Year's Day

Figure 3-10: Holiday One Example Schedule - Added Date in Sorted Order

3. Now update the access control network with the new information. Click on the  button on the tool bar (for details on the update process refer to “Update the Network” on page 35 in section 5).

2.2.2 To Change a Holiday Date

1. To change a holiday date, scroll through the list of holidays and locate the date of the holiday to be changed. Double-click the holiday date field.

*NOTE: When you double-click in the cell, a spinner icon appears (see Figure 3-8 on page 13 of this section). If you click on the month side of the date (**00**/00/00), you can use the spinner to advance the month forward or backward and select the desired month. If you click on the day side of the date (00/**00**/00), you can use the spinner to advance the day forward or backward and select the desired day. If you click on the year side of the date (00/00/**00**), you can use the spinner to advance the year forward or backward and select the desired year. You may decide to use this method to set the date instead of directly typing the information into the cell. Enter the new date for the holiday.*

2. Enter the new holiday date.
3. Click on the 

button. If the holiday schedule is not saved before clicking any other button or exiting the Setup Timezones window, the data entered is lost and must be re-entered. Once the save is complete the holiday schedule is sorted and displayed in order (see Figure 3-10 on page 15 of this section).
4. Now update the access control network with the new information. Click on the 

button on the tool bar (for details on the update process refer to “Update the Network” on page 35 in section 5).

2.3 To Delete a Holiday Schedule

The following instructions explain how to delete the contents of a holiday schedule.

NOTE: Once deleted, a holiday schedule is not recoverable. If a holiday schedule was deleted by mistake, it must be recreated.

NOTE: If a holiday time zone is in use by the access control network, the Doors program will not allow it to be deleted. Review all access groups to ensure all references to the holiday time zone to be deleted have been changed.

1. To delete a holiday schedule you must delete each cell entry one-at-a-time.
2. To delete a date entry, double-click in the date cell. The cursor changes to a cursor. Drag and highlight the entire date entry. Press the **Delete** key.
3. To delete a name entry, double-click in the name cell. The name is automatically highlighted. Press the **Delete** key.
4. Once all dates and names have been deleted (see Figure 3-7 on page 13 of this section), click on the 

button. If the deletions are not saved before clicking any other button or exiting the Setup Timezones window, the deletions are recovered and must be re-deleted.
5. Now update the access control network with the new information. Click on the 

button on the tool bar (for details on the update process refer to “Update the Network” on page 35 in section 5).

3.0 Configure Dedicated I/O Points

This section describes the process for configuring the dedicated input and output points to be used by the system. Certain input/output points on a PXL-250/PXL-500 Controller or SB-293/SB-593 Satellite board are automatically dedicated to input/output functions (i.e. the Door-A RTE input, the Door-A door switch input, the Door-A alarm output, the Door-A lock output). However, if controllers/doors in an access control network need to use the Auxiliary RTE input or need to have separate annunciation of Door Forced and Door Held Open alarms, the inputs and outputs required to perform these functions must be assigned/dedicated to these functions (see Figure 3-11). This will enable the appropriate options within the controllers and doors databases so that these features can be implemented.

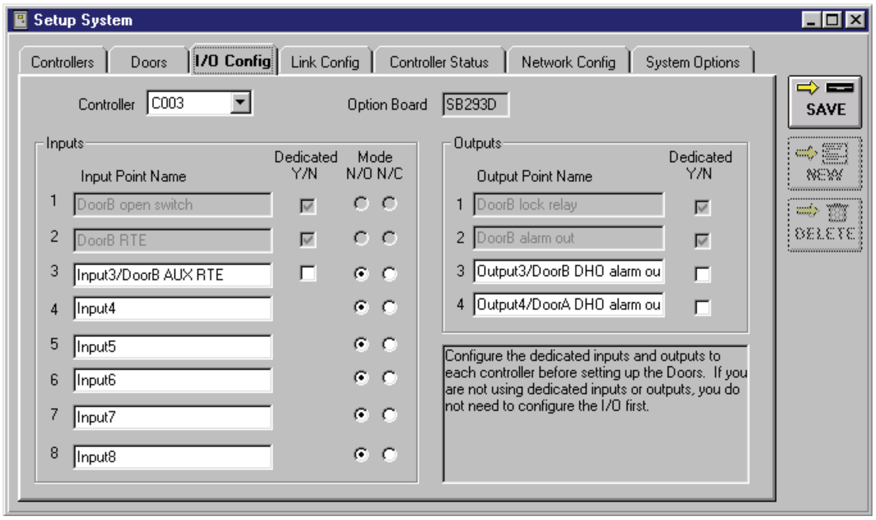


Figure 3-11: Input/Output Points Available for Dedicated Assignment

3.1 Configuring an Auxiliary RTE Input

Auxiliary RTE uses a general purpose input on the PXL-250/PXL-500 Controller or SB-293/SB-593 Satellite board to provide a second RTE input for a door. A typical use for the auxiliary RTE is to allow a receptionist to unlock a door through a switch at the receptionist's desk.

In this example, auxiliary RTE will be configured for Door-B on a controller with a satellite board configured for 2-door control.

1. Click on the Setup ⇒ System pull-down menu or click on the  icon on the tool bar. The Setup System window appears.
2. Click on the **I/O Config** tab. The I/O config window appears (see Figure 3-11 on page 17 of this section).
3. Input points 1 and 2 correspond to the Door-B door switch and to Door-B primary RTE. They are pre-configured and cannot be changed.
4. Input point 3 is available as either a general purpose input point (Input3) or as the auxiliary RTE input for Door-B (DoorB AUX RTE).
5. To configure the point as the auxiliary RTE input, click in the check box in the "Dedicated Y/N" column beside Input Point 3 (see Figure 3-11 on page 17 of this section). When there is a check in the box, the point is dedicated (see Figure 3-12). The name changes to "DoorB AUX RTE" to show the point has been dedicated. To return this point to a general purpose input, click in the check box again and remove the check mark.

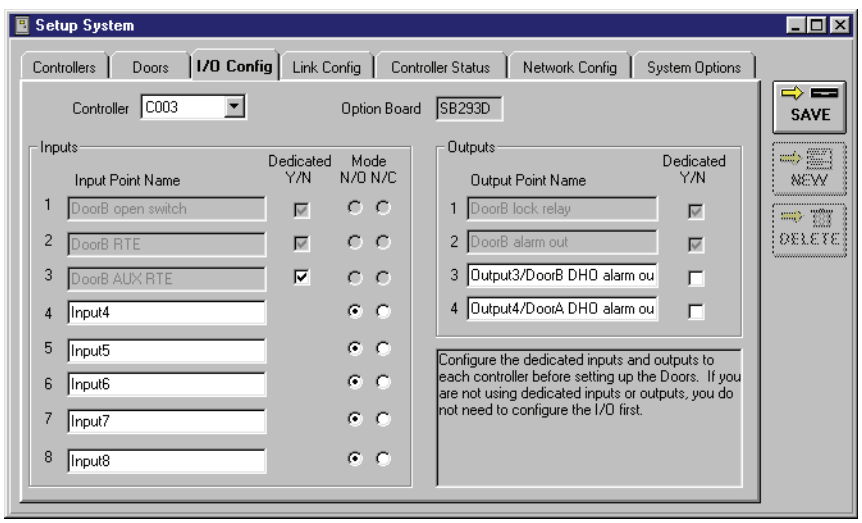


Figure 3-12: Dedicated Input Point

6. Once the point has been configured, click on the  button. If the point configuration is not saved before clicking any other button or exiting the I/O config window, the configuration change does not take affect.

7. Now update the access control network with the new information. Click on the  button on the tool bar (for details on the update process refer to "Update the Network" on page 35 in section 5).

3.2 Configuring Door Held Open Outputs

The Door Held Open (DHO) alarm uses a general purpose output on the SB-293/SB-593 Satellite board to provide separate alarm annunciation for a door held open condition. Output 4 can be assigned as the A-Door DHO alarm and output 3 can be assigned as the B-Door DHO alarm. When DHO is configured, a door forced alarm continues to be annunciated on the original alarm output.

In this example, the DHO output will be configured for Door-B on a controller with a satellite board configured for 2-door control.

1. Click on the Setup ⇒ System pull-down menu or click on the  icon on the tool bar. The Setup/ System window appears.
2. Click on the **I/O Config** tab. The I/O config window appears (see Figure 3-11 on page 17 of this section).
3. Output points 1 and 2 correspond to the Door-B door lock and to the Door-B alarm output. They are pre-configured and cannot be changed.
4. Output point 3 is available as either a general purpose output point (Output3) or as the DHO output for Door-B (DoorB DHO alarm out). (Output point 4 is available as either a general purpose output point or as the DHO output for Door-A. It is not configured in this example).
5. To configure point 3 as the Door-B DHO alarm output, click in the check box in the "Dedicated Y/ N" column beside Output Point 3. When there is a check in the box, the point is dedicated (see Figure 3-13). The name changes to "DoorB DHO alarm out" to show the point has been dedicated. To return this point to a general purpose input, click in the check box again and remove the check mark.

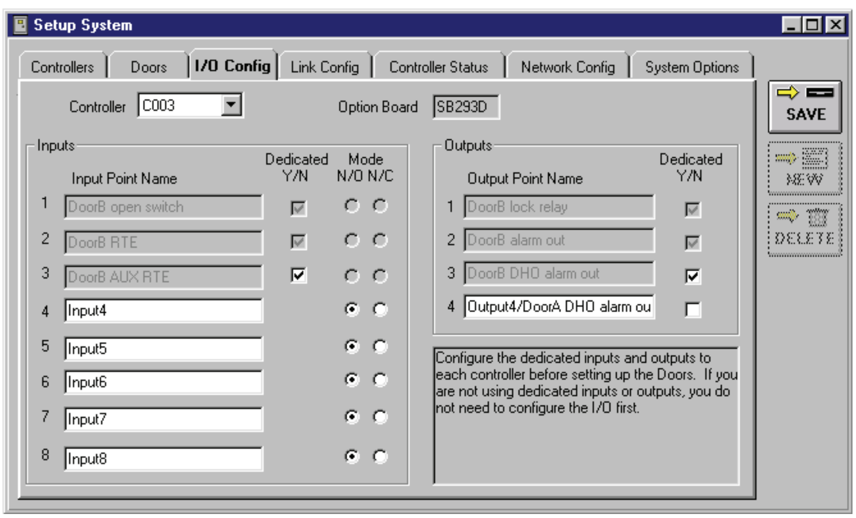


Figure 3-13: Dedicated Output Point

6. Once the point has been configured, click on the  button. If the point configuration is not saved before clicking any other button or exiting the I/O config window, the configuration change does not take affect.

7. Now update the access control network with the new information. Click on the  button on the tool bar (for details on the update process refer to "Update the Network" on page 35 in section 5).

4.0 Setup Controllers/Doors

The setup controllers/doors section describes how to configure controllers and doors on the access control network. The following operations are performed in this section.

Controller Configuration
- set controller dial-out parameters
- enable/disable anti passback
- set a PXL-250W/PXL-500W's Wiegand reader type (LED control)

Door Configuration
- assign a descriptive door name
- assign a door class
- assign a door type
- assign a usage reader type
- enable/disable access through a door
- set a door's unlock time
- set a door's open time
- set a door's unlock/lock time zone
- set a door's first person in value
- set a door's door forced and door held open alarm output modes
- set a door's primary and auxiliary RTE configuration

NOTE: It is not necessary to update the network following each step. However, in order for any changes made to be applied to the network, an update must be completed.

4.1 Controller Configuration

4.1.1 Set Controller Dial-Out Parameters

The dial-out parameters define if a controller is allowed to automatically connect to the host computer and upload its contents to the host computer when the controller's event memory reaches a defined percentage of being full. Each controller has an "Event Capacity" which defines the maximum number of events that can be stored by that controller (see Figure 3-14). When the number of events in a controller reaches the "Threshold Percentage" of that capacity the controller will initiate a connection with the host computer and upload the contents of its event buffer.

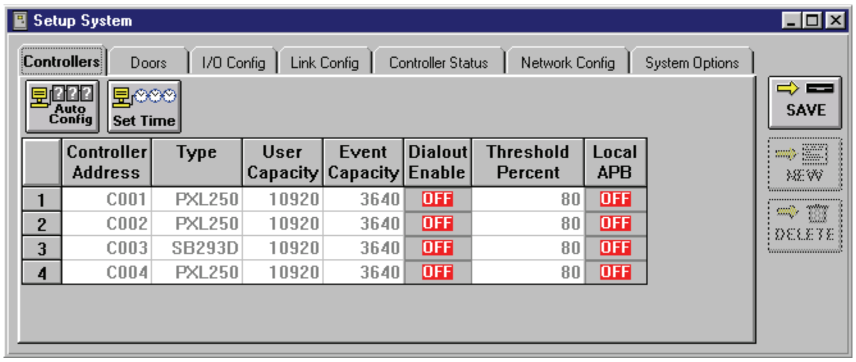


Figure 3-14: Controller Dial-Out Parameters – Disabled

NOTE: These instructions configure the controller for initiating a connection, but the Doors software must also be configured to receive this information. This is done in "Enable/Disable Auto-Collection" on page 4 in section 5. Both steps must be done for proper uploading of information from a controller to the host computer/Doors software.

! ***NOTE: If a controller is not successful in making a connection with the host computer, it will continue to try to make a connection every 10 minutes until a successful connection is made and all data in the controller's buffer is uploaded to the host computer. In order for the controller to be able to connect with the host computer, the host computer must be on and the Doors program must be opened.***

4.1.1.1 Enable Controller Dial-Out

1. To set the controller dial-out parameters, click on the Setup ⇒ System pull-down menu or click on the  tool bar button. Then click on the **Controllers** tab. The Controllers window appears (see Figure 3-14 on page 21 of this section).
2. Scan down the controller addresses column and locate a controller that should have permission to connect to the host computer.
3. Scan across that controller's row in the spreadsheet and locate the **Dialout Enable** button. If the button is , controller dial-out is disabled.
4. To enable controller dialout, click on the **Dialout Enable** button. It will change to  and the text in the "Threshold Percent" column should change color from grey to black (see Figure 3-15). When this text is black, the threshold percent value is editable.

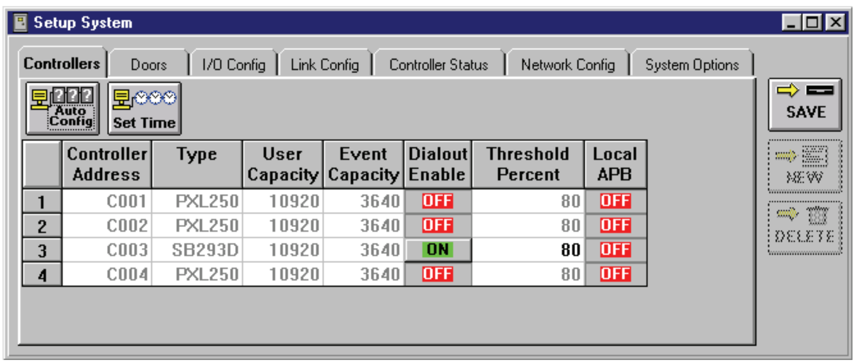


Figure 3-15: Controller Dial-out Parameters – Enabled

5. Once changes have been made, click on the  button. If the changes are not saved before clicking any other button or exiting the system setup window, the data entered is lost and must be re-entered.
6. Now update the access control network with the new information. Click on the  button on the tool bar (for details on the update process refer to "Update the Network" on page 35 in section 5).

4.1.1.2 Set the Dial-Out Threshold Percentage

1. The default value for how full the controller's event buffer should be before connecting to the host computer is 80%. If this value should be changed, to 60% for example, click in the corresponding "Threshold Percent" cell and type **60**. Now, when the controller's event buffer reaches 60% of full, the controller will connect to the host computer and upload the contents of its event buffer.
2. Once changes have been made, click on the  button. If the changes are not saved before clicking any other button or exiting the system setup window, the data entered is lost and must be re-entered.
3. Now update the access control network with the new information. Click on the  button on the tool bar (for details on the update process refer to "Update the Network" on page 35 in section 5).

4.1.1.3 Disable Controller Dial-Out

1. To disable the controller dial-out parameters, click on the Setup ⇒ System pull-down menu or click on the  tool bar button. Then click on the **Controllers** tab. The Controllers window appears (see Figure 3-15 on page 22 of this section).
2. Scan down the controller addresses column and locate a controller that should **not** have permission to initiate a connection with the host computer.
3. Scan across that controller's row in the spreadsheet and locate the **Dialout Enable** button. If the button is 

, controller dial-out is enabled.
4. To disable controller dialout, click on the **Dialout Enable** button. It will change to 

and the text in the "Threshold Percent" column should change color from black to gray (see Figure 3-14 on page 21 of this section). When this text is gray, the threshold percent value is not editable.
5. Once changes have been made, click on the 

button. If the changes are not saved before clicking any other button or exiting the system setup window, the data entered is lost and must be re-entered.
6. Now update the access control network with the new information. Click on the 

button on the tool bar (for details on the update process refer to "Update the Network" on page 35 in section 5).

4.1.2 Enable/Disable Anti Passback

The Local APB button allows an operator to enable/disable the anti passback feature for a reader. Refer to “Set Local Anti Passback” on page 13 in section 2 for more information regarding local anti passback.

1. To enable anti passback, click on the Setup ⇒ System pull-down menu or click on the tool bar button. Then click on the **Controllers** tab (see Figure 3-15 on page 22 of this section).
2. Scan down the “Controller Address” column and locate the controller which should have local APB enabled.
3. Locate the “Local APB” column and click on the OFF button corresponding to the selected controller. The OFF button will toggle to ON and its color will change from red to green. In this example, locate controller address C003 and click on the OFF button.
4. The resulting window should look similar to Figure 3-16.

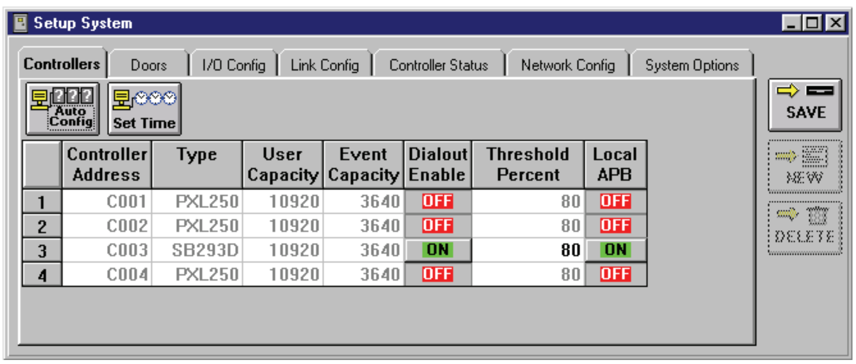
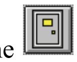


Figure 3-16: Local Anti Passback is ON

5. Disabling local APB is simply the opposite of enabling local APB. Locate the controller to have APB disabled. Click on the ON button in the “Local APB” column corresponding to the selected controller. The ON button will toggle to OFF and its color will change from green to red.
6. Once changes have been made, click on the SAVE button. If the changes are not saved before clicking any other button or exiting the system setup window, the data entered is lost and must be re-entered.
7. Now update the access control network with the new information. Click on the UPDATE NET button on the tool bar (for details on the update process refer to “Update the Network” on page 35 in section 5).

4.1.3 Set Wiegand Reader Type (LED Control)

The Set Wiegand Reader Type field allows an operator to set the type of LED control used by the Wiegand device(s) attached to the controller (reader 1 and/or reader 2). This provides the *Doors* software with the information needed to properly control the Wiegand reader's LED. The *Doors* software recognizes three different ways to control the LED: Single Line, Dual Line, and Essex Keypad.

1. To set the Wiegand reader type, click on the Setup ⇒ System pull-down menu or click on the  tool bar button. Then click on the **Controllers** tab. If the "Reader Wiegand Type" columns do not appear in the window, use the scroll bar at the bottom of the window and scroll to the right until the columns appear (see Figure 3-17).

NOTE: The network is able to determine whether or not you are connected to a Wiegand type reader. If you are not using any Wiegand readers, these columns will not appear.

2. Scroll down the list of controllers and locate the Wiegand controller that has readers to be configured.
3. Scan across the row and locate the Reader 1 Wiegand Type or Reader 2 Wiegand Type column (as appropriate) and click on the  in that cell. A list with the three LED control types appears: Single Line, Dual Line, and Essex Keypad.
4. If that reader is an Essex Keypad, select that type. If not, the reader must be either Single Line or Dual Line. Review the manual for the Wiegand reader and determine the number of LED control lines used by the device. If one LED control line is used, select Single Line. If two LED control lines are used, select Dual Line. In the following example (see Figure 3-17) reader 1 has been set to Dual Line and reader 2 has been set to Essex Keypad.

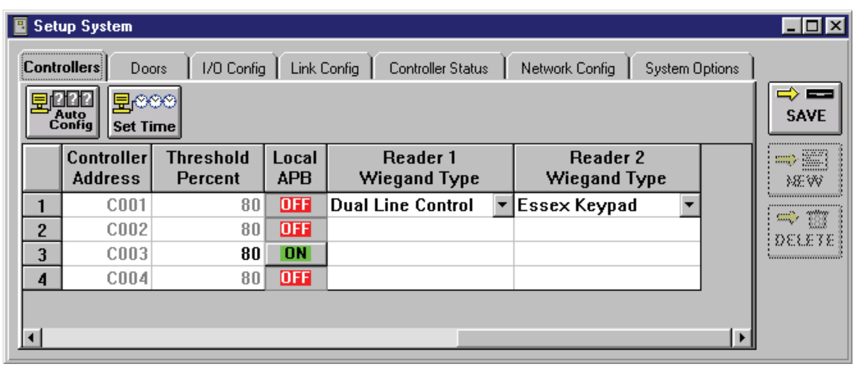


Figure 3-17: Set Wiegand Reader Types

5. Once changes have been made, click on the 

button. If the changes are not saved before clicking any other button or exiting the system setup window, the data entered is lost and must be re-entered.

6. Now update the access control network with the new information. Click on the 

button on the tool bar (for details on the update process refer to "Update the Network" on page 35 in section 5).

4.2 Door Configuration

Door configuration information is assigned under the Setup ⇒ System ⇒ Doors tab. The first time the Doors tab is entered a Configure Dedicated I/O reminder window appears (see Figure 3-18). Refer to "Configure Dedicated I/O Points" on page 17 of this section if you haven't yet configured the dedicated I/O points. Several door configuration options depend upon the values of the dedicated I/O points. Click on the  button to acknowledge the reminder window.

NOTE: When the alarm control feature has been enabled, additional columns appear for configuration of the readers (see "Alarm Control" on page 1 in section 12).

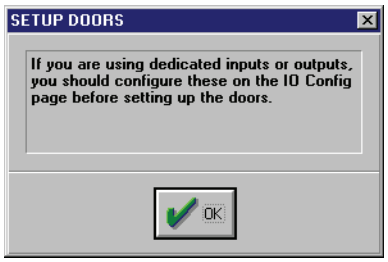
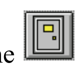


Figure 3-18: Setup Dedicated I/O Points Reminder Window

4.2.1 Assign a Door Name

The door name parameter allows an operator to assign a descriptive name to a door on the access control system. When monitoring system activity or reviewing event reports, it can be easier to follow a string of events if the door associated with the events has a descriptive name.

NOTE: Door names must be 30 characters or less.

1. To assign a door name, click on the Setup ⇒ System pull-down menu or click on the  tool bar button. Then click on the **Doors** tab. The Setup Doors window appears (see Figure 3-19).

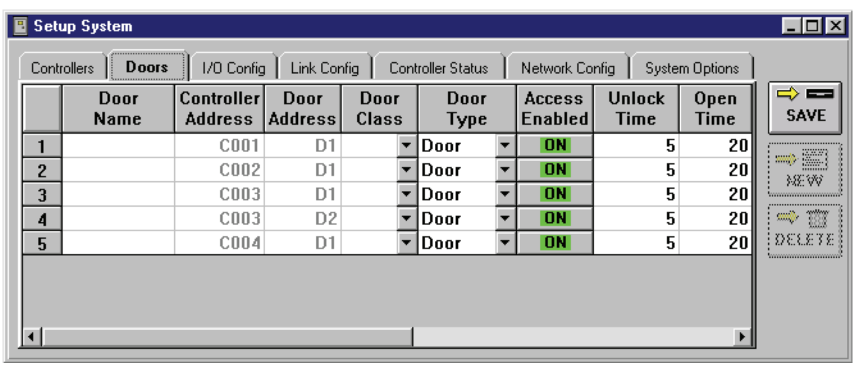


Figure 3-19: Setup Doors Tab - Part 1

2. Scan down the controller/door addresses column and locate a door to be named.
3. Click on the "Door Name" cell corresponding to the selected controller/door address.
4. Type a descriptive name for that door.
5. Scroll through the remaining doors available and give each a descriptive name. The resulting window should look similar to Figure 3-20 on page 27 of this section.

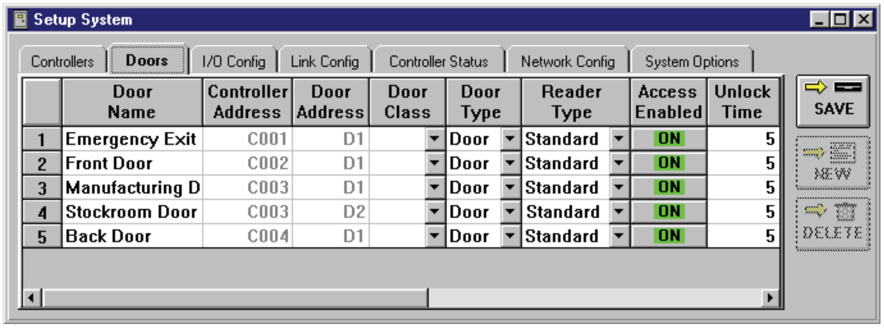


Figure 3-20: Naming Doors

6. Once all the doors have been named, click on the  button. If the changes are not saved before clicking any other button or exiting the system setup window, the data entered is lost and must be re-entered.

4.2.2 Assign a Door Class

Door classes allow an operator to classify doors so that door commands can be performed on all doors within that class. With these classifications in place, an operator can perform commands on door classes such as manually locking/unlocking all doors within the door class or performing a complete database update of all controllers within the door class.

Before assigning door classes, take some time and map out all the door class possibilities for the site. Consider how doors with similar access responsibilities can be grouped together. For example, you could have three door classes: exterior doors, interior doors, and emergency doors. It is important to remember that each door may be assigned to only one door class.

1. To assign a door class, click on the Setup ⇒ System pull-down menu or click on the tool bar button. Then click on the **Doors** tab (see Figure 3-20 on page 27 of this section).
2. Scan down the door name and controller/door address columns and locate a door to be assigned a door class.
3. Click on the "Door Class" cell corresponding to the selected controller/door.
4. Type a descriptive door class title for that door in the "Door Class" cell.

NOTE: In the door class cell is a drop-down arrow . If you click on the arrow, a list with all available selections will appear. Once a number of selections has been entered as described in step 4, you may decide to use this method to quickly enter a selection instead of directly typing the information into the cell.

5. The resulting window should look similar to Figure 3-21.

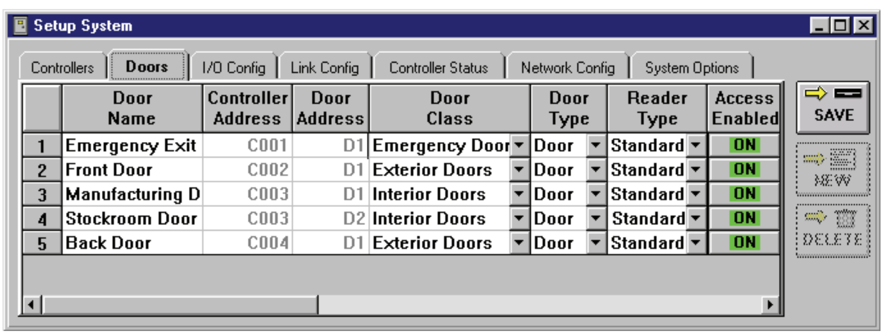


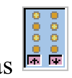
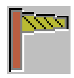
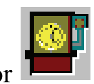
Figure 3-21: Assigning Door Classes

6. Once all the doors have been assigned a door class, click on the SAVE button. If the changes are not saved before clicking any other button or exiting the system setup window, the data entered is lost and must be re-entered.

4.2.3 Assign a Door Type

Door types allow an operator to identify the type of door being used. There are four door types.

- Door – a standard door (default setting)
- Elevator – an elevator door
- Gate – an electric gate (such as a gate controlling a parking lot)
- Time and Attendance Terminal – to be used with a Time and Attendance Terminal

If you turned on the Elevator, Gate, or Time and Attendance Terminal control feature during "Set Door Type" on page 17 in section 2, you need to assign that door type to a specific door at this time. Doors, Gates, and Time and Attendance Terminals are treated exactly the same by the *Doors* program (except when it comes to the exporting of information). The only difference noted by the program is in the icon displayed to identify the door. The standard icon for doors, viewed as , changes to appear as  for doors identified as an elevator,  for doors identified as a gate, or  for doors identified as a Time and Attendance Terminal when creating Access Groups (see "Setup Access Groups" on page 44 in section 3) or when performing manual door control (see "Lock, Unlock, Suspend and Restore Doors" on page 3 in section 6).

NOTE: In order for the Time and Attendance Terminal feature to work properly with the Export feature, make sure the Time and Attendance Terminal has been assigned the door type of Time and Attendance Terminal.

NOTE: A door controlled by an EntraGuard panel is treated the same as a regular door and does not need to be assigned a door type other than Door.

1. To assign a door type, click on the Setup ⇒ System pull-down menu or click on the tool bar button. Then click on the **Doors** tab (see Figure 3-21 on page 28 of this section).
2. Scan down the door name and controller/door address columns and locate a door to be assigned a door type.
3. Scan across the row and locate the "Door Type" column.

NOTE: If you did not choose to use an elevator door, gate, or Time and Attendance Terminal during the doors setup (see "Assign a Door Type" on page 29 in section 3), this column will not appear as an option.

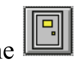
4. Click on the arrow and a list of available door types appears. Scroll up and down this list and select the desired door type.
5. Once changes have been made, click on the SAVE button. If the changes are not saved before clicking any other button or exiting the system setup window, the data entered is lost and must be re-entered.

NOTE: A two-door controller must NOT be configured with one door as an elevator door and the other door as either a regular door or gate. This ensures that proper event filtering of elevator events can be performed (see "Elevator Reports Events" on page 23 in section 5).

4.2.4 Assign a Reader Type (Usage)

The Reader Type (Usage) column allows an operator to identify the specific use of the reader. There are four reader type options.

- Standard – used as a standard reader (default setting)
- In – used to control access into a secure area
- Out – used to control access out of a secure area
- Muster – used to track if someone has arrived at a specific location (used in connection with the Rollcall/Track feature)

1. To assign a reader type, click on the Setup ⇒ System pull-down menu or click on the  tool bar button. Then click on the **Doors** tab (see Figure 3-21 on page 28 of this section).
2. Scan down the door name and controller/door address columns and locate a door to be assigned a reader type.
3. Scan across the row and locate the "Reader Type" column.
4. Click on the  arrow and a list of available usage reader types appears. Scroll up and down this list and select the desired usage reader type.

NOTE: An EntraGuard controller should always be set for Standard usage.

5. Once changes have been made, click on the 

button. If the changes are not saved before clicking any other button or exiting the system setup window, the data entered is lost and must be re-entered.

4.2.5 Disable/Enable Access Through a Door

The access enabled button allows an operator to disable/enable access through a specific door. In normal operation, a door is enabled to allow cards/User IDs to be processed by the controller. However, there may be times when access through a door must be disabled.

NOTE: Even if access through a door is disabled, exit is still allowed through Request to Exit commands, and the door is still monitored for forced openings.

1. To disable/enable access through a door, click on the Setup ⇒ System pull-down menu or click on the tool bar button. Then click on the **Doors** tab (see Figure 3-21 on page 28 of this section).
2. Scan down the door name and controller/door address columns and locate the door to have access disabled.
3. Scan across the row and locate the "Access Enabled" column and click on the ON button corresponding to the selected controller/door (this is the default value). The ON button will toggle to OFF.
4. The resulting window should look similar to Figure 3-22.

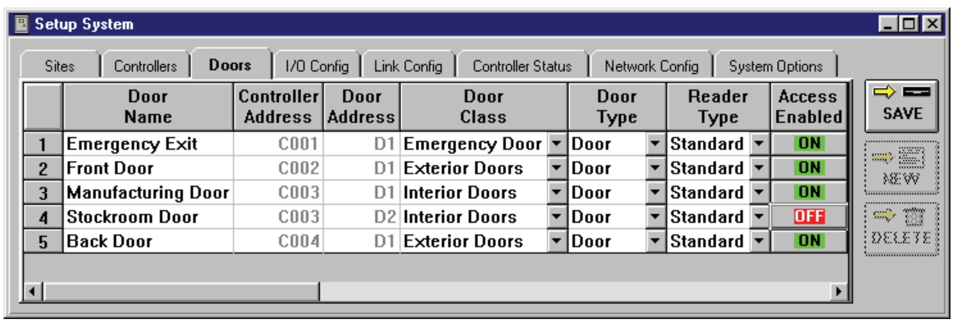


Figure 3-22: Disabling/Enabling Access Through a Door

5. Enabling access through a door is simply the opposite of disabling access through a door. Locate the door to have access enabled. Click on the OFF button corresponding to the selected controller/door. The OFF button will toggle to ON. The window should again appear similar to the window in Figure 3-21 on page 28 of this section.
6. Once changes have been made, click on the SAVE button. If the changes are not saved before clicking any other button or exiting the Setup System window, the data entered is lost and must be re-entered.
7. Now update the access control network with the new information. Click on the UPDATE NET button on the tool bar (for details on the update process refer to "Update the Network" on page 35 in section 5).

4.2.6 Set a Door Unlock Time

The door unlock time is the number of seconds the controller holds the door lock relay in the unlocked position to allow entrance or exit. A timer with this unlock value begins counting once the card is presented to the reader. When the timer ends or the door closes, whichever occurs first, the door lock relay resets to the locked position; the default time is 5 seconds (the door lock also resets when the door is opened if a door status switch is attached to the door and is wired to the controller). For example, a back door through which people carrying packages might pass might need to stay unlocked longer than other doors.

NOTE: The door unlock time is not in addition to the door open time. The door unlock time begins when a card is presented to the reader and ends when the time specified has expired or the door closes, whichever occurs first.

1. To set a door's unlock time, click on the Setup ⇒ System pull-down menu or click on the tool bar button. Then click on the **Doors** tab. If the "Unlock Time" column does not appear in the window, use the scroll bar at the bottom of the window and scroll to the right until the column appears (see Figure 3-23).

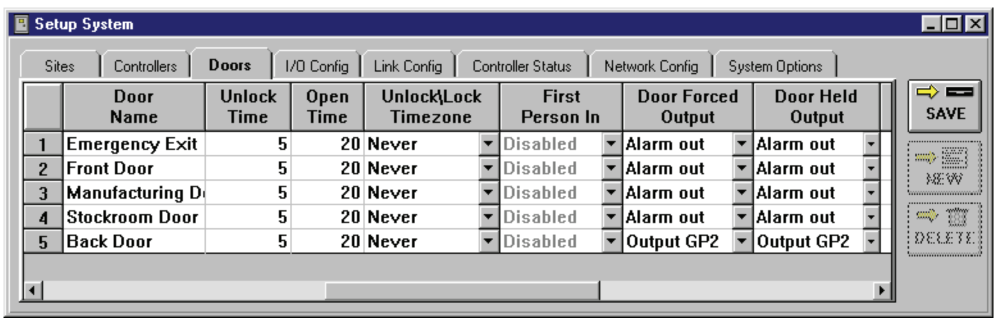


Figure 3-23: Setup Doors Tab - Part 2

2. Scan down the door name and controller/door address columns and locate the door to have an unlock time assigned.
3. Scan across the row and locate the "Unlock Time" column and click on the cell corresponding to the selected controller/door. Type the desired unlock time; the existing value will be overwritten.

NOTE: If you double-click in the cell, a spinner icon will appear. If you click on the spinner icon, you can use the spinner to advance the time forward or backward and select the desired time. You may set it for any amount of time between 1-255 seconds. You may decide to use this method to set the time instead of directly typing the information into the cell.

4. The resulting window should look similar to Figure 3-24 on page 33 of this section.

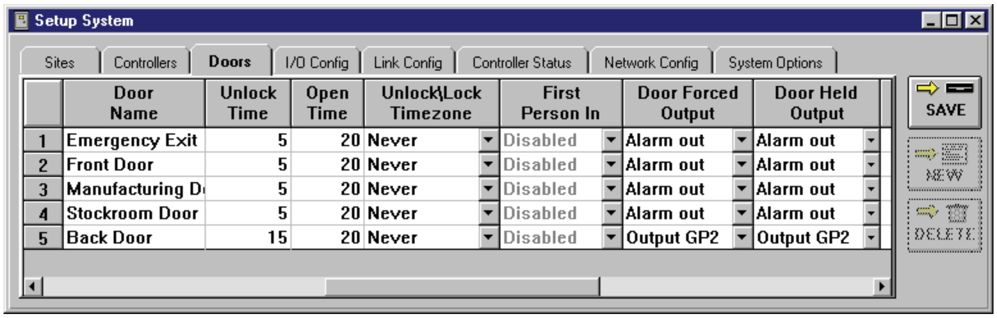


Figure 3-24: Set the Door Unlock Time

5. Once changes have been made, click on the 

button. If the changes are not saved before clicking any other button or exiting the Setup System window, the data entered is lost and must be re-entered.

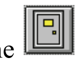
6. Now update the access control network with the new information. Click on the 

button on the tool bar (for details on the update process refer to “Update the Network” on page 35 in section 5).

4.2.7 Set a Door Open Time

The door open time is the number of seconds a door can be held open for entrance or exit before the controller generates a door held alarm. The default time is 20 seconds. For example, a back door through which people carrying packages might pass might need to be held open longer than other doors.

NOTE: The door open time is not in addition to the door unlock time. The door open time begins when the door is opened and ends when the time specified has expired.

1. To set a door's open time, click on the Setup ⇒ System pull-down menu or click on the  tool bar button. Then click on the **Doors** tab (see Figure 3-24 on page 33 of this section). If the "Open Time" column does not appear in the window, use the scroll bar at the bottom of the window and scroll to the right until the column appears.
2. Scan down the door name and controller/door address columns and locate the door to have an open time assigned.
3. Scan across the row and locate the "Open Time" column and click on the cell corresponding to the selected controller/door. Type the desired open time; the existing value will be overwritten.

NOTE: If you double-click in the cell, a  *spinner icon will appear. If you click on the spinner icon, you can use the spinner to advance the time forward or backward and select the desired time. You may set it for any amount of time between 1-255 seconds. You may decide to use this method to set the time instead of directly typing the information into the cell.*

4. The resulting window should look similar to Figure 3-25.

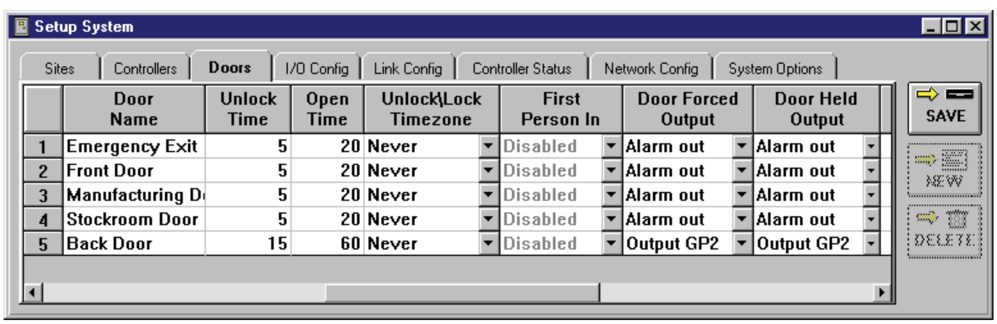


Figure 3-25: Set the Door Open Time

5. Once changes have been made, click on the  button. If the changes are not saved before clicking any other button or exiting the Setup System window, the data entered is lost and must be re-entered.

6. Now update the access control network with the new information. Click on the  button on the tool bar (for details on the update process refer to "Update the Network" on page 35 in section 5).

4.2.8 Set an Unlock/Lock Time Zone

The unlock/lock time zone allows an operator to assign a time zone to a door for the automatic unlocking and locking of that door based on the time zone. For example, a time zone can be created for use by a front door used by customers. The unlock/lock time zone would unlock the front door at the beginning of the time zone and lock it at the end of the time zone. The Unlock/Lock time zones may be Suspended for a time and Restored by the operator. For more information on how to Suspend/Restore the Unlock/Lock time zone see “Suspend/Restore Auto Unlock/Lock” on page 14 in section 6.

1. To set a door’s unlock/lock time zone, click on the Setup ⇒ System pull-down menu or click on the  tool bar button. Then click on the **Doors** tab (see Figure 3-25 on page 34 of this section). If the “Unlock/Lock Timezone” column does not appear in the window, use the scroll bar at the bottom of the window and scroll to the right until the column appears.
2. Scan down the door name column and locate the door to have an unlock/lock time zone assigned.
3. Locate the “Unlock/Lock Timezone” column and click on the cell corresponding to the selected controller/door.
4. Click on the ▾ arrow and a list of available time zones will appear. Scroll up and down this list and locate the desired time zone. For example, if a “Customer TZ” time zone has been created (see “Setup Time Zones” on page 3 of this section) allowing access between 08:00 and 17:00 (8 A.M. and 5 P.M.), click on the **Customer TZ** timezone.
5. The resulting window should look similar to Figure 3-26.

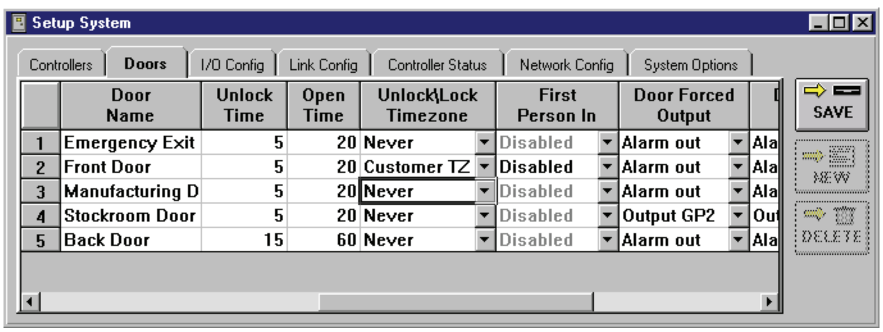


Figure 3-26: Set the Unlock/Lock Timezone

6. Once changes have been made, click on the  button. If the changes are not saved before clicking any other button or exiting the Setup System window, the data entered is lost and must be re-entered.

7. Now update the access control network with the new information. Click on the  button on the tool bar (for details on the update process refer to “Update the Network” on page 35 in section 5).

NOTE: The unlock/lock timezone is valid on holidays as well as days-of-the-week. Any door assigned an unlock/lock timezone that includes a holiday schedule will be automatically unlocked and locked on the dates in that holiday schedule (see “Holiday Schedules” on page 12 of this section).

4.2.9 First Person In

First Person In (FPI) allows an operator to determine if a door should be automatically unlocked when the unlock/lock time zone begins, or if the door should not automatically unlock for the unlock/lock time zone until after a person presenting a valid card arrives. The default value for FPI is DISABLED, meaning the FPI feature is not applied. To use FPI it must be enabled.

FPI can be used wherever employees may be delayed in arriving at a secured site (perhaps due to inclement weather). This ensures that at least one access-granted employee is in the building before the unlock/lock time zone is allowed to unlock the door for general entrance/exit.

There are five alternate values that may be selected:

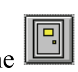
- ENABLED
- ENABLED 15
- ENABLED 30
- ENABLED 45
- ENABLED 60

The ENABLED value simply enables FPI beginning when the unlock time of the unlock/lock time zone is reached. The ENABLED XX values allow a controller to “look ahead” 15, 30, 45, or 60 minutes. If an employee presents a valid card during the look ahead period, the door will unlock and allow that employee access (but still will not unlock for general access until the time specified by the unlock/lock time zone). This allows access for an employee who arrives to work early. If this feature is used, the operator should select a time that best suits the security needs of the site.

NOTE: Before setting an FPI value for a door, verify the time zone associated with that door is a time zone other than Always or Never. If the Always time zone is selected, the door will never be locked; if the Never time zone is selected, FPI cannot be applied.

NOTE: When considering applying FPI to a door, remember the unlock/lock time zone assigned to the door may have more than one start/stop time period (up to a maximum of four). If FPI is applied to a door, it applies to each start/stop time period in the door’s unlock/lock time zone.

NOTE: If the Auto Unlock/Lock time zone has been Suspended (see “Suspend/Restore Auto Unlock/ Lock” on page 14 in section 6), First Person In is disabled.

1. To set a door’s FPI value, click on the Setup ⇒ System pull-down menu or click on the  tool bar button. Then click on the **Doors** tab (see Figure 3-26 on page 35 of this section). If the “First Person In” column does not appear in the window, use the scroll bar at the bottom of the window and scroll to the right until the column appears.
1. Scan down the door name and controller/door address columns and locate the door to which an FPI value should be assigned.
2. Locate the “First Person In” column and click on the cell corresponding to the selected controller/ door.
3. Click on the  arrow and a list of FPI values will appear. Scroll up and down this list and locate the desired FPI value. For example, click on the “**ENABLED 60**” FPI value.
4. The resulting window should look similar to Figure 3-27 on page 37 of this section.

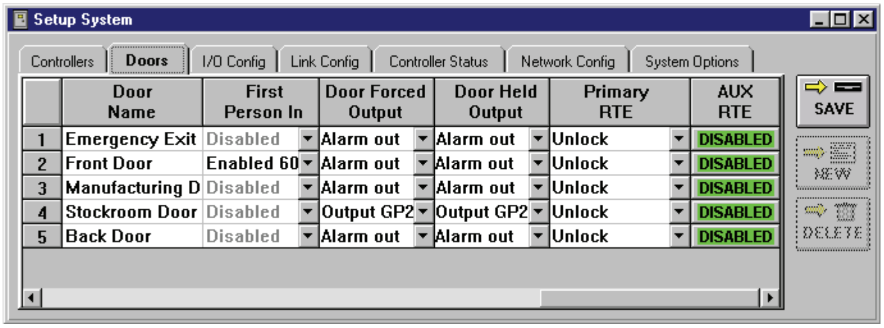


Figure 3-27: Set the First Person In Value

5. Once changes have been made, click on the 

button. If the changes are not saved before clicking any other button or exiting the Setup System window, the data entered is lost and must be re-entered.

6. Now update the access control network with the new information. Click on the 

button on the tool bar (for details on the update process refer to "Update the Network" on page 35 in section 5).

4.2.10 Door Forced and Door Held Alarm Outputs

The Door Forced and Door Held alarm outputs allow an operator to select the alarm annunciation mode for door forced alarms and door held alarms.

A Door Forced alarm is activated whenever the door associated with the alarm output is forced open. A Door Held Open alarm is activated whenever the door associated with the alarm output is held open beyond the door open time period. When an alarm is activated it will remain on until the alarm condition is corrected; a forced door must be closed and a door held open must be closed. Depending upon the configuration of the controller, there are several options for configuring which alarms are annunciated at which relays.

4.2.10.1 PXL Controller by Itself

PXL controllers have only one alarm output relay. All alarm outputs are annunciated through this relay. The door forced alarm can be annunciated through the alarm relay or be disabled (a door forced alarm will not be annunciated by the relay). The door held alarm can be annunciated through the alarm relay or be disabled (a door held alarm will not be annunciated by the relay).

Door Forced Output

1. To set the door forced and door held alarm output values, click on the Setup ⇒ System pull-down menu or click on the  tool bar button. Then click on the **Doors** tab (see Figure 3-27 on page 37 of this section). If the "Door Held Output" column does not appear in the window, use the scroll bar at the bottom of the window and scroll to the right until this column appears.
2. Scan down the door name column and locate the door to have alarm output values assigned.
3. Locate the "Door Forced Output" column and click on the cell corresponding to the selected door.
4. Click on the  arrow and a list of available alarm output values appears. Scroll through this list and select the desired door forced output value. Alarm Out is the default value for this field.

Door Held Open Output

1. To set the door forced and door held alarm output values, click on the Setup ⇒ System pull-down menu or click on the  tool bar button. Then click on the **Doors** tab (see Figure 3-27 on page 37 of this section). If the "Door Forced Output" column does not appear in the window, use the scroll bar at the bottom of the window and scroll to the right until this column appears.
2. Scan down the door name column and locate the door to have alarm output values assigned.
3. Locate the "Door Held Output" column and click on the cell corresponding to the selected door.
4. Click on the  arrow and a list of available alarm output values appears. Scroll through this list and select the desired door held output value. Alarm Out is the default value for this field.

4.2.10.2 PXL with a Satellite Board (SB) Configured in 2-Door Mode

Satellite Boards add output relays that can be dedicated to separate annunciation of door forced and door held alarms. When a Satellite board is configured for 2-door operation, two of the board’s four relays are automatically configured for the second door lock and alarm output annunciation. The remaining two relays are eligible to be dedicated to the other alarm annunciation functions, allowing door forced alarms to be separated from door held alarms for both doors.

NOTE: To have separate annunciation of door forced and door held alarms, the output relay points must have been dedicated to alarm annunciation. This process is described in “Configure Dedicated I/O Points” on page 17 in section 3.

Table 1 summarizes the options available to a PXL with a Satellite Board configured for 2-door operation.

Table 1: Alarm Annunciation Options PXL/Satellite Board

	Door Forced	Door Held	Comment
A-Door	Disabled	Disabled	no alarm annunciation
	Alarm Out relay on PXL	Alarm Out relay on PXL	Door Held alarm is annunciated with Door Forced alarm
		GP 4 Output on SB (dedicated output point)	Door Held alarm is annunciated at its own alarm relay
B-Door	Disabled	Disabled	no alarm annunciation
	GP 2 Output on SB (default Alarm Out relay)	GP 2 Output on SB (default Alarm Out relay)	Door Held alarm is annunciated with Door Forced alarm
		GP 3 Output on SB (dedicated output point)	Door Held alarm is annunciated at its own alarm relay

For example, A-Door and B-Door are configured in 2-Door mode.

- The A-Door needs to be monitored for just the door forced condition.
- The B-Door needs to be monitored for **both** door forced and door held open conditions on separate alarm outputs.

A-Door

1. To set the door forced and door held alarm output values, click on the Setup ⇒ System pull-down menu or click on the  tool bar button. Then click on the **Doors** tab. If the “Door Forced Output” and “Door Held Output” columns do not appear in the window, use the scroll bar at the bottom of the window and scroll to the right until these columns appear.
2. To set the A-Door alarm output, scan down the door name column and locate the door to have alarm output values assigned.
3. Locate the “Door Forced Output” column and click on the cell corresponding to the selected door.

4. Click on the  arrow and a list of available alarm output values appears. Scroll through this list and locate the desired door forced output value. For this example, click on **Alarm Out**.
5. Locate the “Door Held Output” column and click on the cell corresponding to the selected door.
6. Click on the  arrow and a list of available alarm output values appears. Scroll through this list and locate the desired door held output value. For this example, click on **Disabled**.

B-Door

1. To set the door forced and door held alarm output values, click on the Setup ⇒ System pull-down menu or click on the  tool bar button. Then click on the **Doors** tab. If the “Door Forced Output” and “Door Held Output” columns do not appear in the window, use the scroll bar at the bottom of the window and scroll to the right until these columns appear.
2. To set the B-Door alarm output, scan down the door name column and locate the door to have alarm output values assigned.
3. Locate the “Door Forced Output” column and click on the cell corresponding to the selected door.
4. Click on the  arrow and a list of available alarm output values appears. Scroll through this list and locate the desired door forced output value. For this example, click on **Output GP2**.
5. Locate the “Door Held Output” column and click on the cell corresponding to the selected door.
6. Click on the  arrow and a list of available alarm output values appears. Scroll through this list and locate the desired door held output value. For this example, click on **Output GP3**.
7. The resulting window should look similar to Figure 3-28.

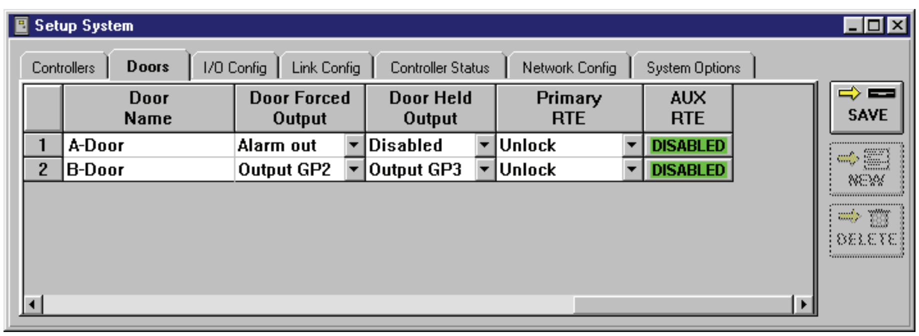


Figure 3-28: Set the Alarm Output Values

8. Once changes have been made, click on the  button. If the changes are not saved before clicking any other button or exiting the Setup System window, the data entered is lost and must be re-entered.
9. Now update the access control network with the new information. Click on the  button on the tool bar (for details on the update process refer to “Update the Network” on page 35 in section 5).

4.2.11 Primary/Auxiliary Request to Exit

The Request to Exit (RTE) input accepts a signal from a normally open input device such as a push button. A signal from this device indicates a request has been made for someone to exit through a secured door. Push buttons, motion detectors, floor mats, or similar devices can provide the RTE signal. When the controller receives an RTE signal, it operates the door based on the controller's RTE configuration.

A request to exit can be made in two ways: through the primary RTE input and through the auxiliary RTE input. On a PXL controller, primary RTE is requested through the controller's RTE input (the standard implementation) and auxiliary RTE is requested through the controller's general purpose input.

On a controller with a Satellite Board configured for 2-door control, the RTE options for the A-door (attached to the controller) apply as described above. Primary RTE for the B-door is requested through the satellite board's RTE input (the standard implementation) and auxiliary RTE for the B-door is requested through general purpose input 3 on the satellite board.

NOTE: If the auxiliary RTE feature is enabled on the master controller (including an EntraGuard controller), the Global Unlock feature (see "Set Network Master Parameters" on page 10 in section 2) is automatically disabled. Both features use the same input so only one of these two features can be used on the master controller.

There are three door configuration options for primary RTE.

- Disabled – There is no request to exit function at all. Exit is not allowed through that door via RTE.
- Do Not Unlock – The request to exit is recorded and the door held open timer starts, but the door must manually be opened for exit (typically the door has a manual door strike, crash bar or similar device).
- Unlock – The request to exit is recorded, the door held open timer starts, and the door unlock relay unlocks the door to allow exit.

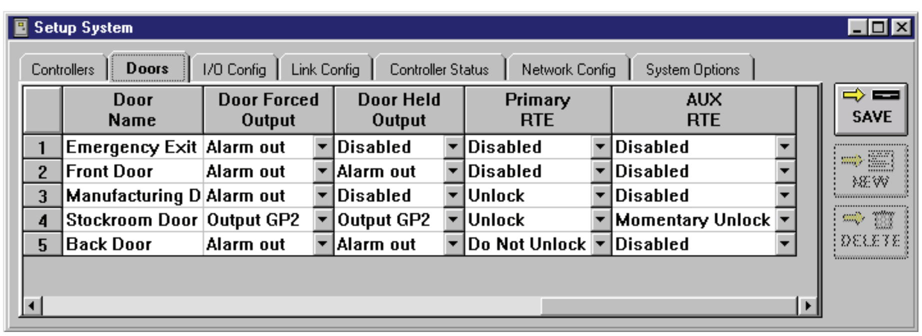
There are three door configuration options for auxiliary RTE: Disabled, Momentary Unlock, and Continuous Unlock.

- Disabled – There is no request to exit function at all. Exit is not allowed through that door via RTE.
- Momentary Unlock – The request to exit is recorded, the door held open timer starts, and the door unlock relay unlocks the door to allow exit.
- Continuous Unlock (CRTE) – The request to exit is recorded and any assigned Auto Unlock/Lock (AUL) time zone is Suspended for a given door. Then, while the CRTE input is active, the door is unlocked. When CRTE becomes inactive, the door will assume its AUL time zone configuration state.

The default value for primary RTE is Unlock; the default for auxiliary RTE is Disabled. For example:

- The Emergency Exit does not use the RTE feature. Both primary and auxiliary RTE should be set to Disabled.
- The Manufacturing Door uses the primary RTE input. Primary RTE should be set to Unlock and auxiliary RTE should be set to Disabled.
- The Stockroom Door uses both the primary and auxiliary RTE input. Primary RTE should be set to Unlock and auxiliary RTE should be set to Momentary Unlock.
- The Back Door uses the primary RTE input, but should not automatically unlock the back door. Primary RTE should be set to Do Not Unlock. Auxiliary RTE should be set to Disabled.

1. To set the primary and auxiliary RTE values, click on the Setup ⇒ System pull-down menu or click on the tool bar button. Then click on the Doors tab (see Figure 3-28 on page 40 of this section. If the “Primary RTE” and “AUX RTE” columns do not appear in the window, use the scroll bar at the bottom of the window and scroll to the right until these columns appear.
2. Scan down the door name column and locate the door to have primary and auxiliary RTE values assigned.
3. Locate the “Primary RTE” column and click on the cell corresponding to the selected door.
4. Click on the arrow and a list of available RTE values appears. Scroll through this list and select the desired RTE value. For this example, click on Disabled. The default value for auxiliary RTE is Disabled, so this value does not need to be changed.
5. Repeat steps 2 through 4 for the Front Door. The Manufacturing Door is already set at the default values and does not need to change.
6. Scan down the door name column and locate the door to have primary and auxiliary RTE values assigned: Stockroom Door.
7. Primary RTE is already set at the default value and does not need to change.
8. Locate the “AUX RTE” column and click on the cell corresponding to the selected door.
9. Click on the arrow and a list of available RTE values appears. Scroll through this list and select the desired RTE value. For this example, click on Momentary Unlock.
10. Scan down the door name column and locate the door to have primary and auxiliary RTE values assigned: Back Door.
11. Locate the “Primary RTE” column and click on the cell corresponding to the selected door.
12. Click on the arrow and a list of available RTE values appears. Scroll up and down this list and locate the desired RTE value. For this example, click on Do Not Unlock. The default value for auxiliary RTE is Disabled, so this value does not need to be changed.
13. The resulting window should look similar to Figure 3-29.



	Door Name	Door Forced Output	Door Held Output	Primary RTE	AUX RTE
1	Emergency Exit	Alarm out	Disabled	Disabled	Disabled
2	Front Door	Alarm out	Alarm out	Disabled	Disabled
3	Manufacturing D	Alarm out	Disabled	Unlock	Disabled
4	Stockroom Door	Output GP2	Output GP2	Unlock	Momentary Unlock
5	Back Door	Alarm out	Alarm out	Do Not Unlock	Disabled

Figure 3-29: Set the Primary and Auxiliary RTE Values

NOTE: When using the Continuous Request to Exit (CRTE), a few rules need to be considered.

- ***A Global Lock and a manual Lock command take precedence over a CRTE request. However, once the Global Lock or manual Lock command has been issued, a subsequent CRTE request will unlock the door.***
- ***A CRTE request takes precedence over an AUL time zone function ONLY if the CRTE request is active before the start time of the time zone and it keeps its precedence as long as the CRTE request stays active.***
- ***If a CRTE request is active when a Global Lock command goes inactive, the door will unlock until the CRTE request goes inactive or until some other Lock command overrides the CRTE request.***
- ***CRTE and Global Unlock are mutually exclusive features; since they share the same input, you can only enable one feature or the other, not both.***

14. Once changes have been made, click on the 

button. If the changes are not saved before clicking any other button or exiting the Setup System window, the data entered is lost and must be re-entered.

15. Now update the access control network with the new information. Click on the 

button on the tool bar (for details on the update process refer to “Update the Network” on page 35 in section 5).

5.0 Setup Access Groups

The setup access groups section provides the instructions for creating access groups. Access groups combine time zones and doors into a superset of information that is applied to users – basically when and where individual users are granted access. Each door can be assigned a unique time zone, or any number of doors can be assigned the same time zone.

To be granted access to a secure door, a user must meet the criteria of the access group. The user must be at a door that accepts members of that access group and it must be during a time zone that allows that user access.

Doors uses a *Windows* convention called a Wizard to create an access group. The access group wizard is a sequential set of windows that requests information from the operator and then creates an access group. This section provides examples for creating a new access group, editing an existing access group, and deleting an access group.

NOTE: Any users assigned access to a reader that has been set up for alarm control use (in connection with a PXL-500/PXL-510 controller and NetworX NX-8E Alarm Panel) will have the ability to affect the alarm system. For further information on use of the alarm control feature, refer to "Alarm Control" on page 1 in section 12.

NOTE: Always close the Access Group Wizard window when you have finished working with access groups before opening another window and starting another operation. This prevents conflicts between Access Group operations and any other operations.

5.1 Create a New Access Group

This section uses an example to describe the process for creating a new access group. In this example, the day shift staff needs access to the front, back, and manufacturing doors during the day shift time zone.

NOTE: It is important that each step in the Access Group creation process be performed in order. Jumping between the Edit Access Group and Save Access Group windows can result in the incorrect Access Group being edited or saved.

1. To create a new access group, click on the Setup ⇒ Access Groups pull-down menu or click on the  tool bar button. The Create and Edit Access Groups window appears (see Figure 3-30).

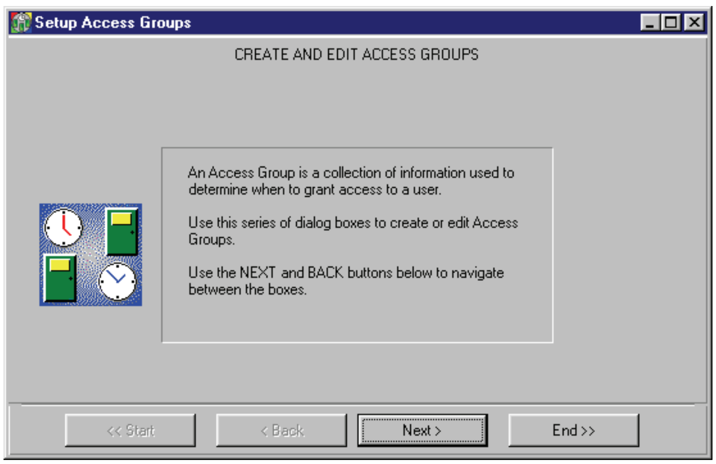


Figure 3-30: Create and Edit Access Groups - Entry Window

2. Click on the 

button and the Edit Access Group window appears (see Figure 3-31).

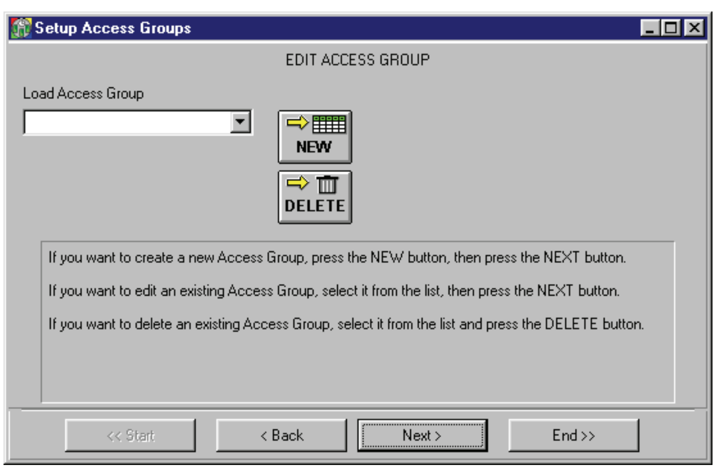


Figure 3-31: Edit Access Group

3. Click on the 

 button. This will clear any information that may be stored in the access group fields.

4. Click on the 

 button and the Select Doors window appears (see Figure 3-32).

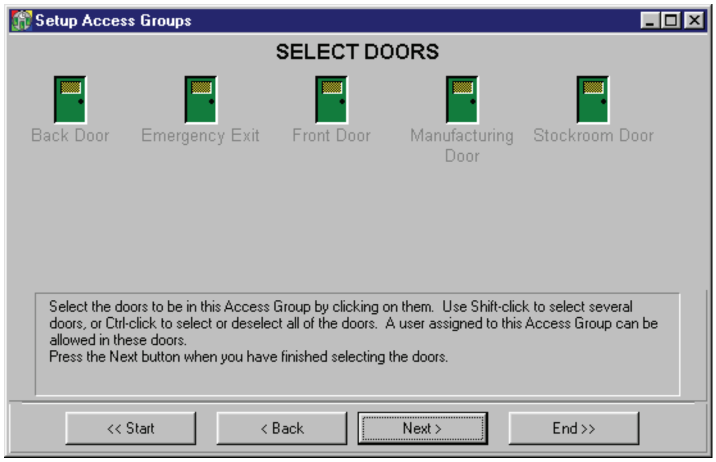


Figure 3-32: Select Doors Window - Available Doors

5. The Select Doors window in Figure 3-32 displays all doors recognized by the system. Click on the doors to be included in this access group. For this example, click on the **Back Door**, **Front Door**, and **Manufacturing Door** icons. The window should look similar to Figure 3-33. If an incorrect door was selected, simply click on that door again. Each click on a door toggles its state between selected and deselected.

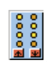
NOTE: If a door has been configured as an elevator door by the Door Type command (see "Assign a Door Type" on page 29 in section 3) its icon appears as *. If a door has been configured as a gate by the Door Type command (see "Assign a Door Type" on page 29 in section 3) its icon appears as* *. The icon for an EntraGuard unit appears as* *.*



Figure 3-33: Assigning Doors to the New Access Group

NOTE: Selected doors can be differentiated from unselected doors by the appearance of the door icon. Selected doors stand out from the window and their door names are written in black text. Unselected doors appear to recede into the window and their door names are written in grey text.

6. Click on the  button and the Assign Timezones window appears (see Figure 3-34).

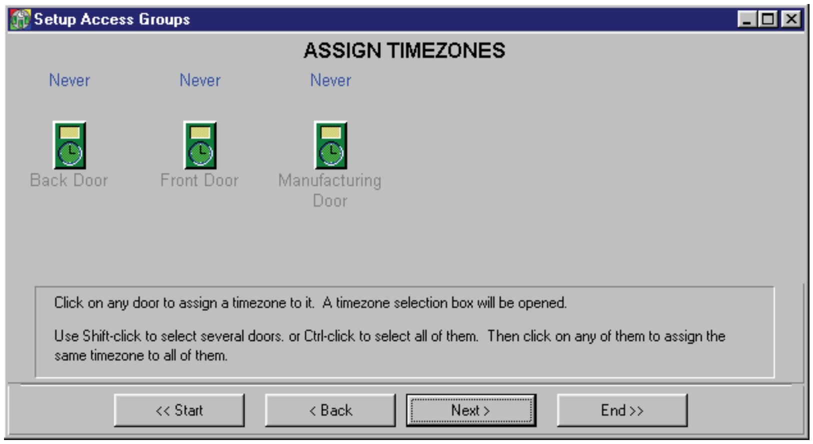


Figure 3-34: Assign Timezones Window - Selected Doors

7. The selected door icons should appear in this window. If a door icon is missing or an unwanted door icon is in the window, click on the Back button to return to the previous window and make the necessary changes.
8. Click on the **Back Door** icon. A time zone list window appears in the middle of the Assign Timezones access group window (see Figure 3-35).

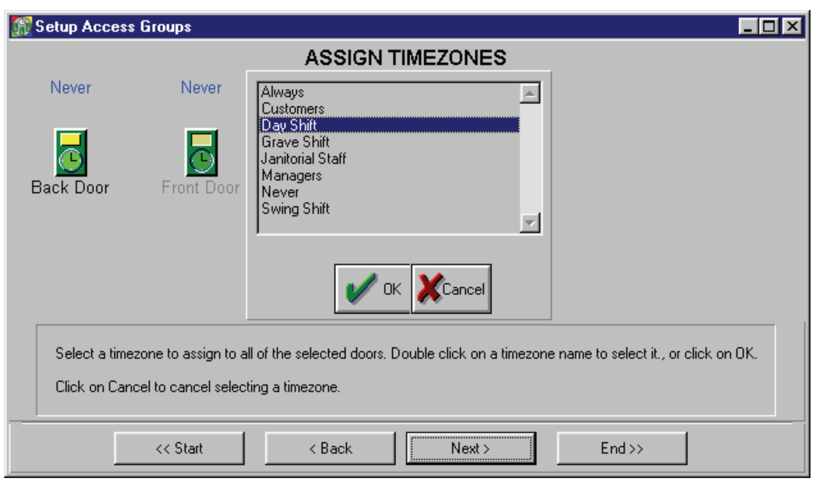
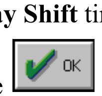


Figure 3-35: Assigning Timezones to Doors in the Access Group

9. Scroll through the timezone window and locate the **Day Shift** time zone.
10. Click on the **Day Shift** time zone and then click on the  button. The time zone list window disappears and the time zone name appears over the door icon.
11. Repeat steps 8 through 10 for the Front Door and the Manufacturing Door.

12. When complete, the access group window should look similar to Figure 3-36 on page 48 of this section.

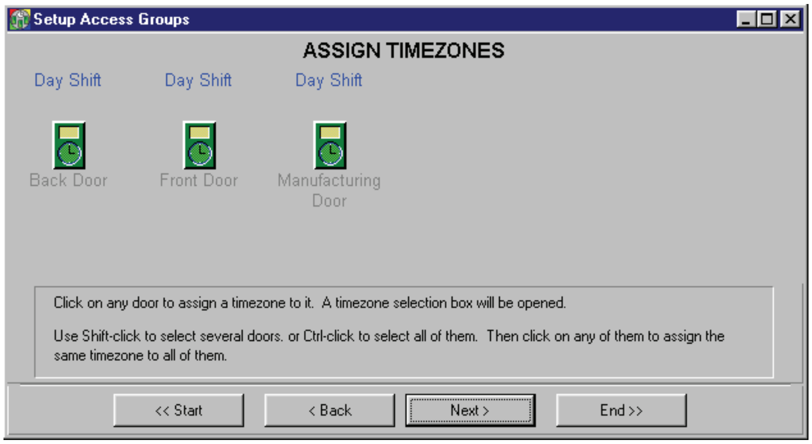


Figure 3-36: Access Group Door/Timezone Assignments

13. Click on the 

button and the Save Access Group window appears (see Figure 3-37).

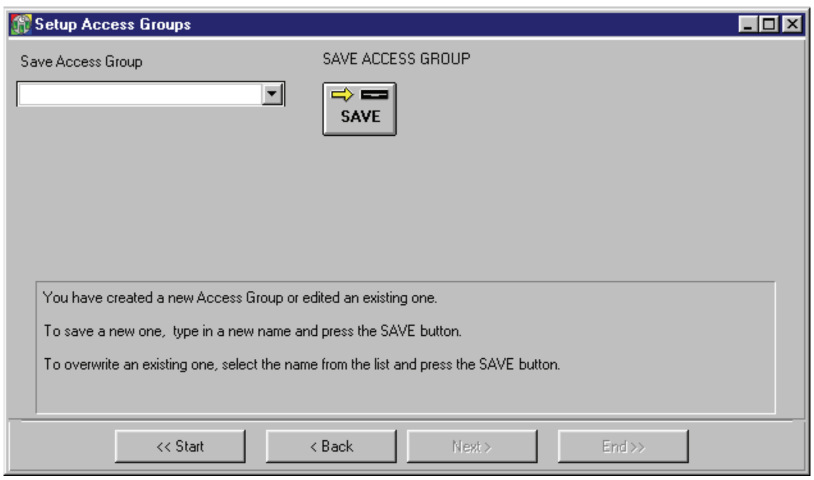


Figure 3-37: Save Access Group Window

14. Click in the “Save Access Group” field and type a descriptive name for this access group. For this example, type **Building Access - Day**. The window should look similar to Figure 3-38 on page 49 of this section.

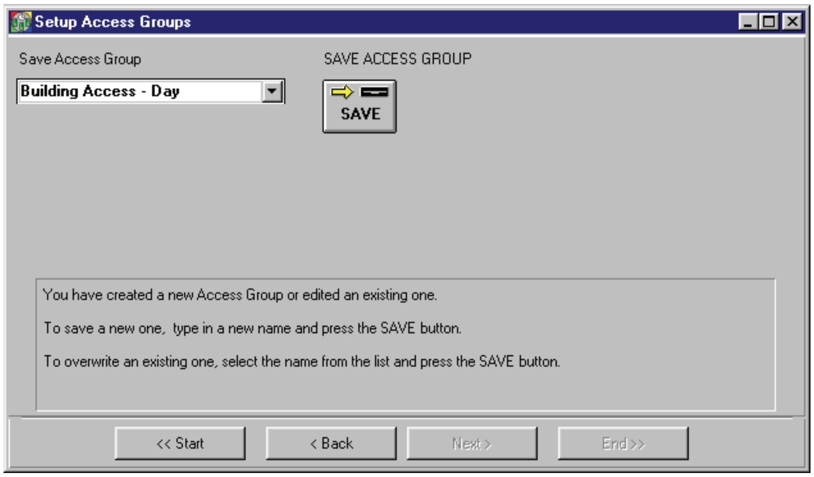


Figure 3-38: New Access Group Saved

15. Click on the  button. If the new access group is not saved before clicking any other button or exiting the setup access group window, the data entered is lost and must be re-entered.
16. Click on the  button to begin entering a new access group.
17. Once you have entered and saved all the access groups, you need to update the access control network with the new information. Click on the  button on the tool bar (for details on the update process refer to “Update the Network” on page 35 in section 5).

5.2 Edit an Existing Access Group

This section describes the process for editing an existing access group. In this example, two changes to a Janitorial Access access group will be made: access to the stockroom will be removed and the front door's time zone assignment will be changed from Day Shift to Janitorial Staff.

NOTE: It is important that each step in the Access Group creation process be performed in order. Jumping between the Edit Access Group and Save Access Group windows can result in the incorrect Access Group being edited or saved.

1. To edit an access group, click on the Setup ⇒ Access Groups pull-down menu or click on the  tool bar button. The Create And Edit Access Groups window appears (see Figure 3-39).

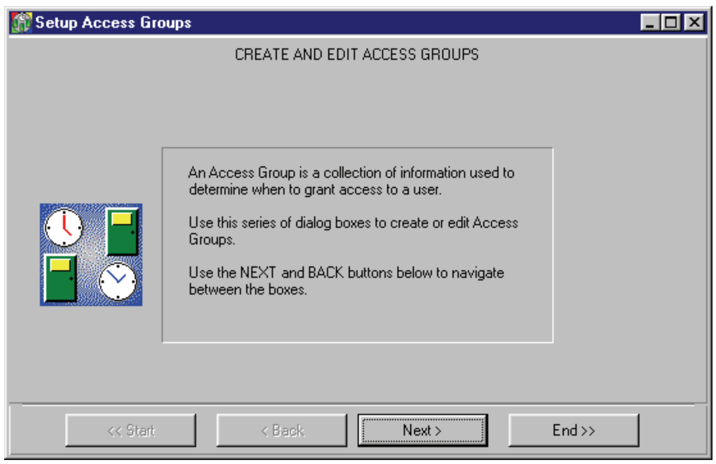


Figure 3-39: Create And Edit Access Groups - Entry Window

2. Click on the 

button and the Edit Access Group window appears (see Figure 3-40).

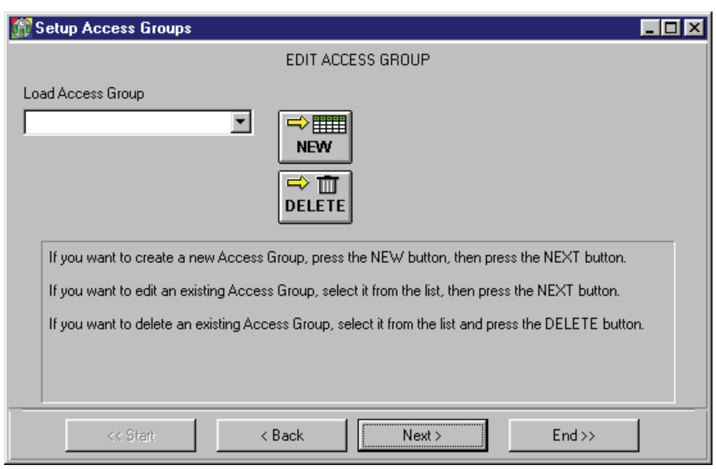


Figure 3-40: Edit Access Group

3. Click on the arrow in the "Load Access Group" field and a list of available access groups will appear. Scroll through this list and select the desired access group for editing (see Figure 3-41 on page 51 of this section).

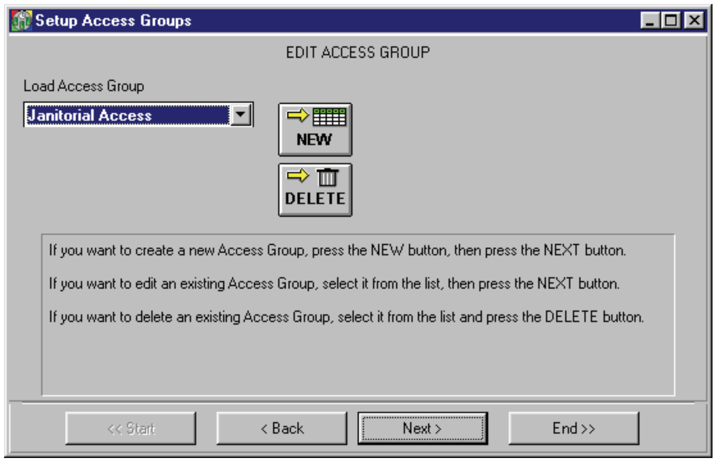


Figure 3-41: Selected Access Group for Editing

4. Click on the Next > button and the Select Doors window appears showing that the Back Door, Front Door, Manufacturing Door, and Stockroom Door are all selected, and that the Emergency Exit is not selected (see Figure 3-42).

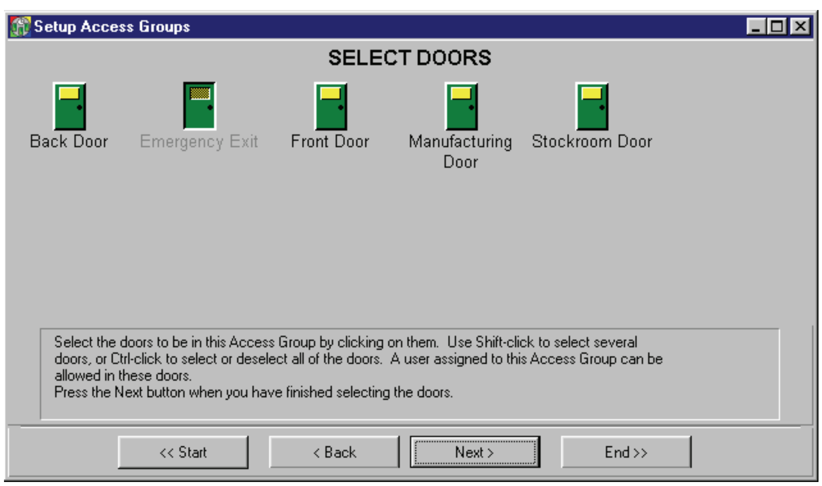


Figure 3-42: Select Access Group Doors for Editing

5.2.1 Add/Remove a Door from the Access Group

1. Continuing on from Figure 3-42 on page 51 of this section using the example of deleting a door from the access group, click on the **Stockroom Door** icon. This will remove the door from the access group. The door icon will change and appear to recede into the window, and the door name text will change from black to grey. The setup access groups window changes to appear similar to Figure 3-43.

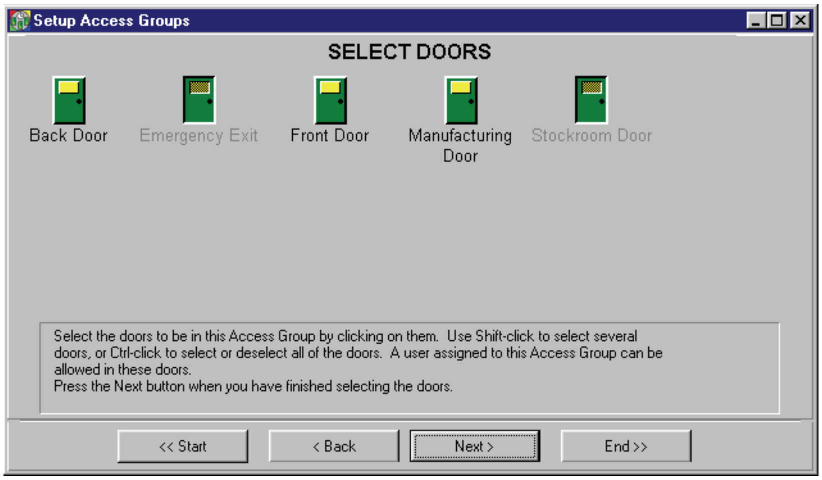


Figure 3-43: Edited Access Group Doors

2. Should a door need to be added to the access group, click on that door icon. This will add the door to the access group. The door will change and appear to stand out from the window, and the door name text will change from grey to black.

3. Once all changes have been made, click on the [Next >] button and the Assign Timezones window appears (see Figure 3-44).

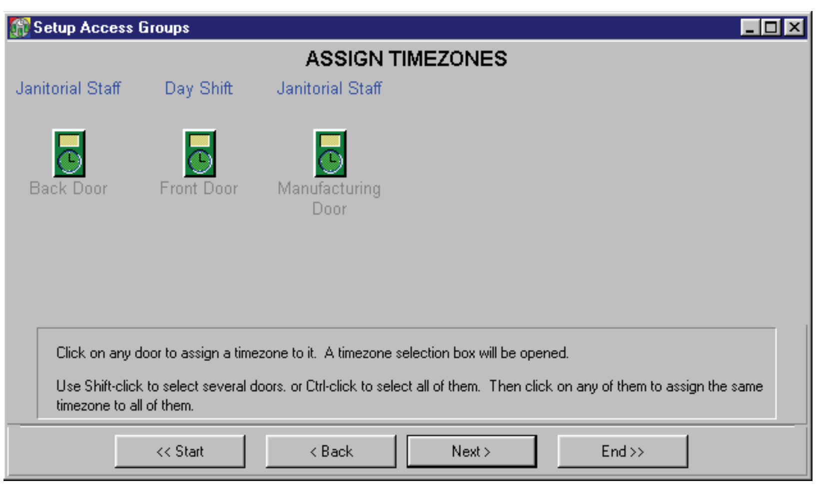


Figure 3-44: Access Group Time Zones for the Edited Doors

4. The correct door icons should now appear in this window. If a wanted door icon is missing or an unwanted door icon is in the window, click on the Back button to return to the window in Figure 3-43 and make the necessary changes.

5.2.2 Change the Time Zone on an Access Group Door

1. Continuing on from Figure 3-44 on page 52 of this section using the example of changing the time zone on an access group door, click on the door to be changed.
2. Click on the **Front Door** icon. A small, time zone list window will appear in the middle of the Assign Timezones window (see Figure 3-45).

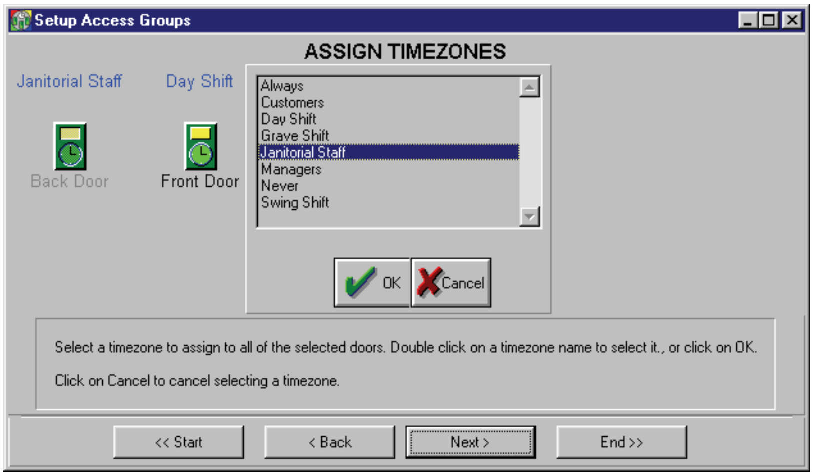


Figure 3-45: Changing Time Zones to Doors in the Access Group

3. Scroll through the time zone window and locate the **Janitorial Staff** time zone.
4. Click on the **Janitorial Staff** time zone and then click on the  button. The time zone list window will disappear and the window should look similar to Figure 3-46.

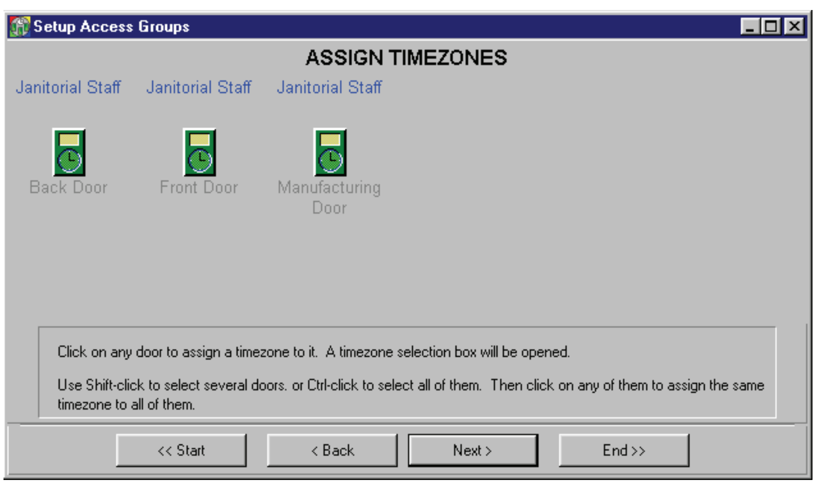


Figure 3-46: Edited Time Zone on Front Door of Access Group

5. Click on the  button and the save Access Group window appears (see Figure 3-47 on page 54 of this section).

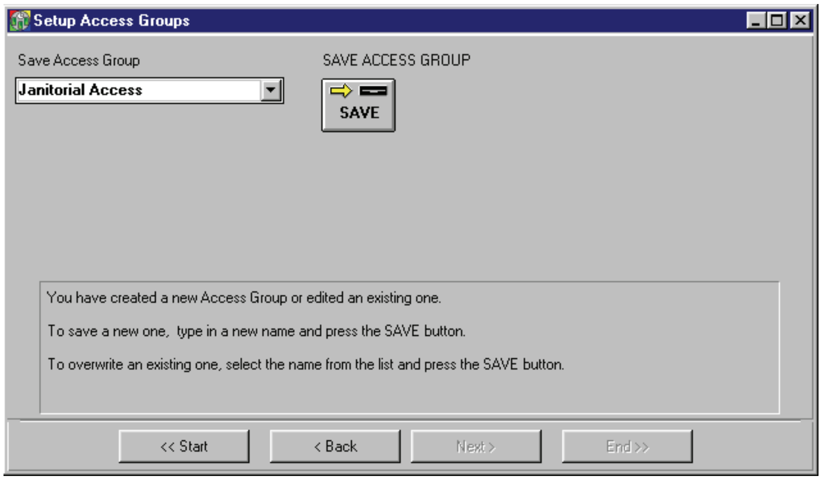


Figure 3-47: Save the Edited Access Group

6. Click on the  button. If the edited access group is not saved before clicking any other button or exiting the Setup Access Groups window, the data entered is lost and must be re-entered.

7. Now update the access control network with the new information. Click on the  button on the tool bar (for details on the update process refer to “Update the Network” on page 35 in section 5).

5.3 Delete an Access Group

This section describes the process for deleting an access group. For this example, an access group named Emergency Access will be deleted.

NOTE: It is important that each step in the Access Group creation process be performed in order. Jumping between the Edit Access Group and Save Access Group windows can result in the incorrect Access Group being edited or saved.

NOTE: If an access group is in use by the access control network, the Doors program will not allow it to be deleted. Review all cardholder/access group assignments to ensure all references to the access group to be deleted have been changed.

1. To delete an access group, click on the Setup ⇒ Access Groups pull-down menu or click on the  tool bar button. The Create and Edit Access Groups window appears (see Figure 3-48).

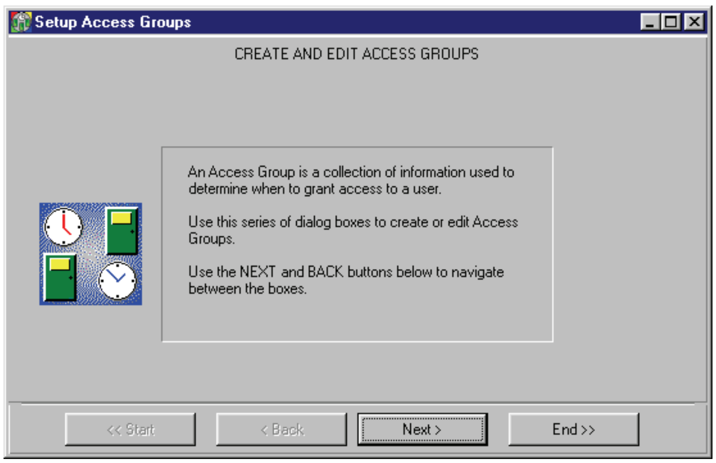


Figure 3-48: Create and Edit Access Groups - Entry Window

2. Click on the  button and the Edit Access Group window appears (see Figure 3-49).

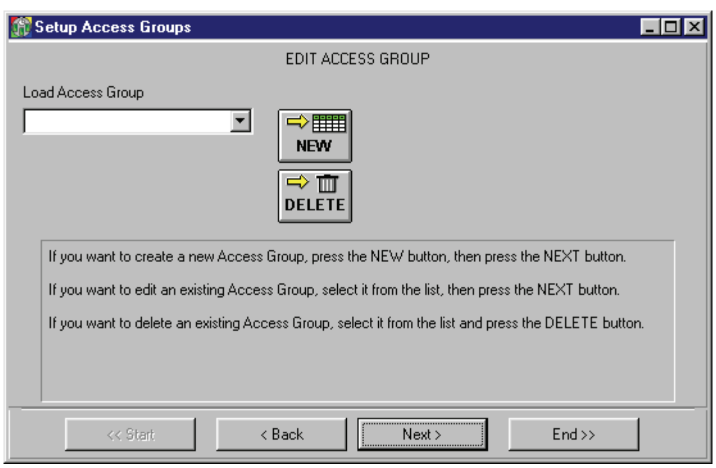


Figure 3-49: Edit Access Group Window

3. Click on the ▼ arrow in the "Access Group Names" field and a list of available access groups will appear. Scroll through this list and locate the desired access group for deleting. For this example, click on the "Emergency Access" time zone and that access group is entered into the "Access Group Names" field (see Figure 3-50).

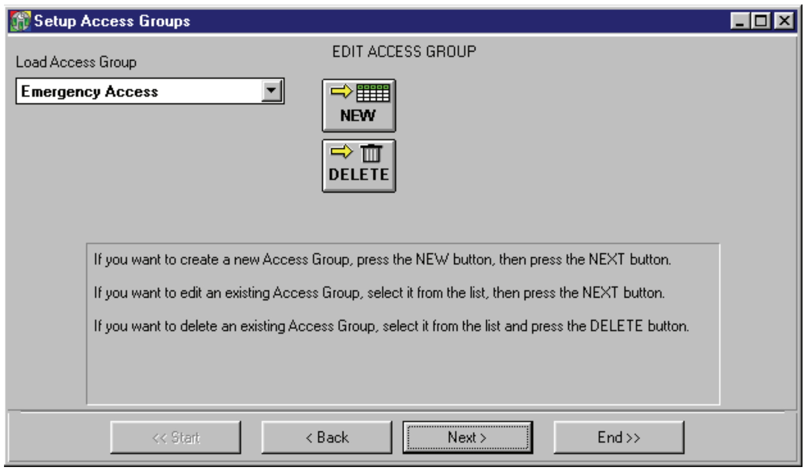


Figure 3-50: Selected Access Group for Deletion

4. Click on the DELETE button. The access group is removed from the system.

5. Click on the SAVE button. If the edited access group is not saved before clicking any other button or exiting the Setup Access Groups window, the data entered is lost and must be re-entered.

6. Now update the access control network with the new information. Click on the UPDATE NET button on the tool bar (for details on the update process refer to "Update the Network" on page 35 in section 5).

Section 4

Setup Users

Each person to be granted access to secured areas will have assigned to them a card, PIN (Personal Identification Number), User ID, or any combination of these that identifies that person to the access control system. The Setup Users section provides the instructions for enrolling access control cards and PINs and managing the database for these.

NOTE: This section does not include enrollment of User IDs to be used in connection with an EntraGuard Telephone Entry unit. For further instructions on enrolling users where an EntraGuard controller is in use or where a mixed EntraGuard/PXL system is in use, see "EntraGuard" on page 1 in section 10.

Through the Setup Users menu, an operator can enroll, void, and delete cards/PINs; assign cards/PINs to users; enter and edit user information, including personal data fields; and apply access groups to users. There are two methods for working with the user database: through dialog boxes or through a spreadsheet. Each method accomplishes the same tasks.

The dialog box method ("User Data – Dialog Box Method" on page 13 of this section) allows an operator to enter all user data through a series of "fill-in-the-blank" type windows. The spreadsheet method (see "User Data – Spreadsheet Method" on page 22 of this section) allows an operator to enter all user data into a spreadsheet. Work with the method that feels the most comfortable to you.

NOTE: The generic term "card" also applies to Keri Systems' PKT-10 key tags.

*NOTE: If you are enrolling cards for a "hybrid" site (one using **both** Proximity and Wiegand cards), enrolling Wiegand cards with different facility codes, or enrolling cards with user-defined card numbers, it is possible to have duplicate card numbers. If desired, after enrollment, the duplicate card numbers can be changed to prevent confusion. The program will not allow cards with identical internal numbers to be enrolled. If you attempt to enroll a card that has an identical internal number with a card already enrolled, it will be rejected.*

Document Number 01914-004, Revision 5.2 – September, 2003

1.0 Card Enrollment

Determine what kind of enrollment is needed for the access control system in use. For example, if you have only PXL controllers being used, then you will need to enroll only cards (Card+PIN would be needed if at least one of those controllers has a P-650 Card+PIN Proximity Reader and Keypad connected to it). For enrollment of User IDs only, or cards and User IDs see “EntraGuard” on page 1 in section 10. For enrollment of Temp User cards, see “Temp Users” on page 1 in section 13. For enrollment of Dual Verification users, see “Dual Verification” on page 1 in section 14.

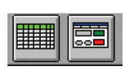
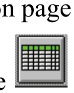
1.1 Block Enrollment by Card Number Range

Block enrollment by card number range is best used when there is a large quantity of sequential ID numbered cards or credentials. This is true for Keri Systems Proximity Cards or for 26-bit Wiegand formatted credentials (such as magnetic stripe, bar code, or keypad readers). Cards or credentials do not have to be on hand when enrolled through the block enrollment by card number range process, but you must have the facility code and they must have sequential ID numbers. For non-Keri Systems, Wiegand formatted credentials, you must work with the manufacturer/supplier of the credentials to ensure that the sequential ID number list you have for the credentials correctly reflects the ID numbers programmed into the credentials.

Block enrollment by card number range is valid for “K” and “W” series Keri Proximity Cards (identified by a “K” or “W” prefix on the number printed on the body of the card). Block enrollment by card number range is not available for “C” series cards or key tags (used by older Keri Systems products).

For proper block enrollment of non-Keri Systems Wiegand formatted credentials, the Wiegand reader and the Wiegand credentials must transfer data in the 26-bit format defined in the Security Industry Association’s Wiegand Interface Standard (document number AC-01D-96) or in the Keri Systems Reference Document Processing Wiegand Format Card Data (P/N 01846-001). Proper enrollment cannot be guaranteed if either the Wiegand reader or the Wiegand credentials do not transfer data in this format.

NOTE: If you are using the Card+PIN feature in connection with the P-650 Card+PIN Proximity Reader and Keypad, and PXL-250W/PXL-500W you must use 26-bit Wiegand cards enrolled through block enrollment.

1. To enroll cards by block enrollment, click on the Setup ⇒ Users pull-down menu or click on the  tool bar button. These two icons  are added to the tool bar and the Setup Users spreadsheet window appears (see Figure 4-1 on page 4 of this section). If the Setup Users spreadsheet window is not visible, click on the  tool bar button.

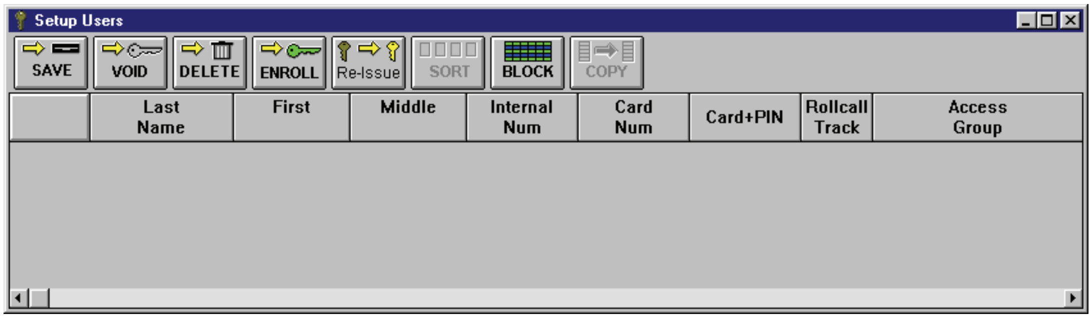


Figure 4-1: Setup Users Spreadsheet Window

2. Click on the  button. If the *Doors* program is not connected to the access control network, the program will automatically connect. The Enroll Cards window appears (see Figure 4-2).

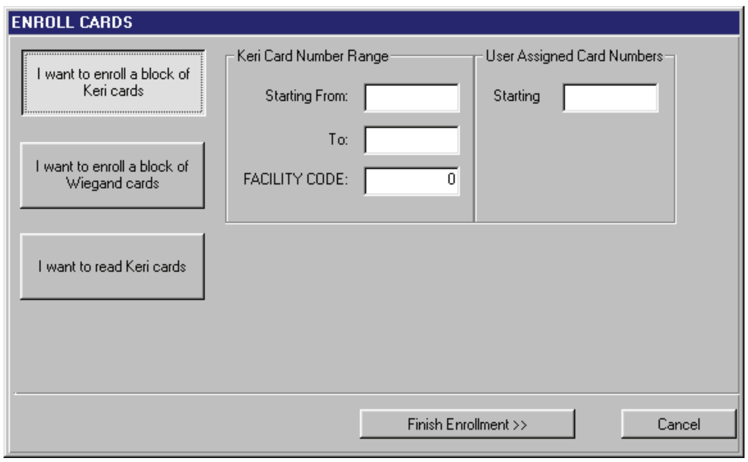
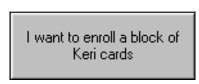
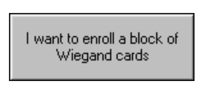


Figure 4-2: Enroll Cards Window

3. If the cards to be enrolled are Keri Proximity cards, click on the  button.

4. If the cards to be enrolled are 26-bit Wiegand cards, click on the  button.

NOTE: If you are using a mixed PXL/EntraGuard system where users need to be given both a card and a User ID, follow the instructions in "EntraGuard" on page 1 in section 10.

5. Locate the Keri/Wiegand Card Number Range field. Click in the **Starting From** field. Enter the card number for the <u>first</u> card in the range of cards to be enrolled (the lowest number). The card number is the second set of digits printed on the body of the card (in Figure 4-3 on page 5 of this section, it is the digits corresponding to 187491). The card number will be more than 4 digits long. For example, the entire number of the first card is K1757 187491; the card number is **187491**, 6 digits long.

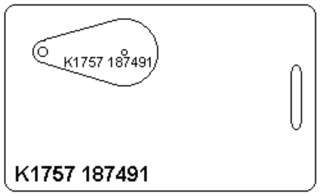


Figure 4-3: Proximity Card/Key Tag Number

6. Locate the Keri/Wiegand Card Number Range field. Click in the **To** field. Enter the card number for the last card in the range of cards to be enrolled (the highest number). The card number is the second set of digits printed on the body of the card (in Figure 4-3, it is the digits corresponding to 187491). The card number will be more than 4 digits long. For example, the entire number of the last card is K1757 187495; the card number is 187495.

7. Locate the Facility Code field. Click in the **FACILITY CODE** field and enter the facility code for the cards. The default facility code value is 0 (zero).

*NOTE: For Keri Proximity cards, facility codes may range from 0 to 31. For 26-bit Wiegand cards, facility codes may range from 0 to 255. The facility code is programmed into each card. To enroll cards, you **must** know the facility code programmed into the card. If you do not know the facility code for the cards you are enrolling, please contact your card supplier for the facility code number **before** continuing the card enrollment process.*

NOTE: If you are block enrolling non-Keri Wiegand cards, be sure you know the actual internal card numbers programmed into the cards and verify the internal numbers are in consecutive order. Using incorrect numbers and non-consecutive cards invalidate the block enrollment process.

8. The default for User Assigned Card Numbers is to copy the card number from the Keri/Wiegand Card Number Range field. If there is a need for user assigned card numbers that are different from the card number printed on the body of the card, locate the User Assigned Card Numbers field. Click in the **Starting** field. Enter the user assigned number for the first card in the set (the lowest number). Numbers for the remaining cards will be assigned in ascending, sequential order from the first number.
9. The resulting window should look similar to Figure 4-4.

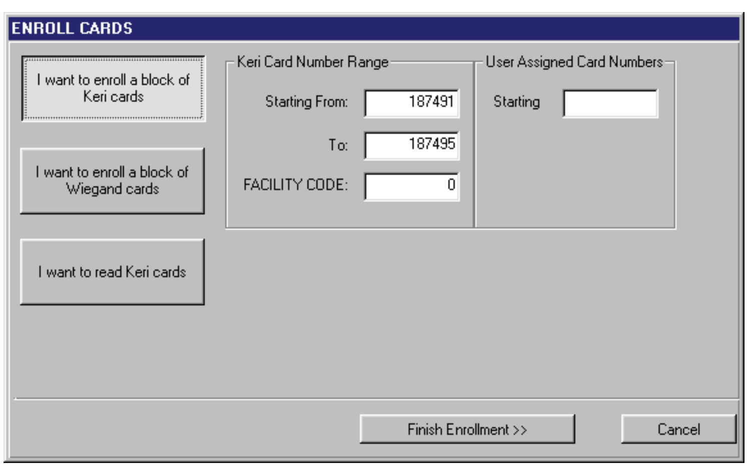
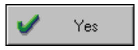


Figure 4-4: Enroll Cards Window – Block Enrollment

10. Click on the 

button.

NOTE: If a large number of cards are being enrolled (greater than 5,000 cards at one time), it can take some time for the enrollment process to complete. A card quantity verification window appears (see Figure 4-5) to warn the operator of the time involved in enrolling a large number of cards at one time.

Click on the 

button to continue with the enrollment. If the number of cards being enrolled is incorrect, or if you do not want to enroll such a large number of cards at one time, click on the 

button.

NOTE: Entering a large amount of cards by mistake (i.e 30,000) may be more than the host computer is able to handle.

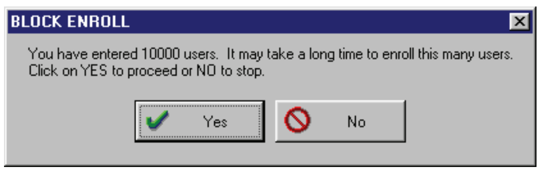


Figure 4-5: Block Enrollment Card Quantity Verification Window

11. The Enroll New Users window displays a confirmation of enrollment (see Figure 4-6).

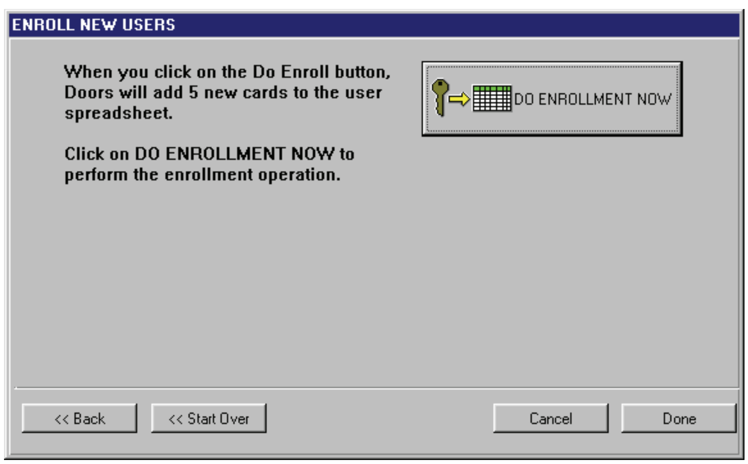
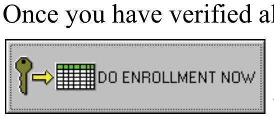


Figure 4-6: Enroll New Users Confirmation Window

12. The confirmation display shows the number of cards you are about to enroll. Take a moment to verify this number is correct. If this number is incorrect, click on the 

button or the 

button to return to the Enroll Cards window to make changes.
13. Once you have verified all the information is correct on the confirmation display, click on the 

button. The cards are enrolled and the Enroll New Users window displays the enrollment results (see Figure 4-7 on page 7 of this section).

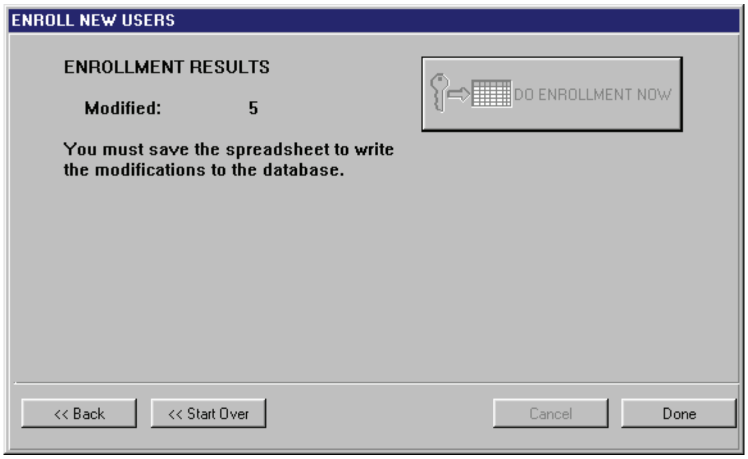


Figure 4-7: Enrollment Results Window

14. Carefully examine the information displayed under Enrollment Results. This field will alert you to the number of cards successfully enrolled and if there were any duplicates.

NOTE: If more than 100 cards are being enrolled at one time, the enrollment results display will show the enrollment of cards increase in increments of 100 until the database slots for all cards being enrolled have been created.

15. Click on the 

button to close the Enroll New Users window. The Setup Users spreadsheet window now contains the newly enrolled cards (see Figure 4-8).

NOTE: If you are enrolling 26-bit Wiegand cards to be used with the Card+PIN feature, and have selected the Card+PIN option in "Set Card+PIN (P-650) Mode" on page 22 in section 2, the card PIN is automatically generated and placed in the Card+PIN column of the Setup Users spreadsheet.

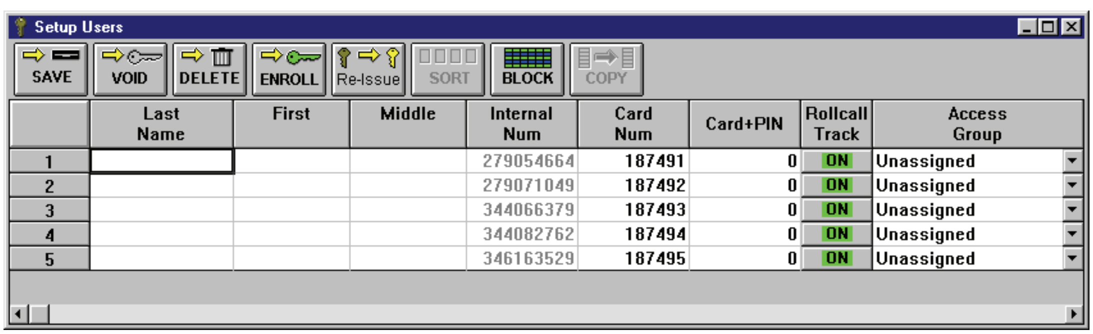


Figure 4-8: Setup Users Spreadsheet Window With Block Enrolled Cards

16. Click on the 

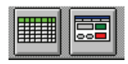
button to save the enrollment. If the card enrollment information is not saved before clicking any other button or exiting the Setup Users window, the data entered is lost and must be re-entered.

1.2 Enrollment by Presenting to a Reader

Enrolling by presenting to a reader is best used when there are only a few cards to enroll or the cards are not in sequential order. The cards must be on hand to be enrolled by presenting to a reader. The “A” reader on a Proximity master controller is the enrollment reader. However, on a Wiegand master controller, the “A” reader, “B” reader, or both readers may be used as the enrollment reader.

! ***NOTE: If you are using the Card+PIN feature in connection with the P-650 Card+PIN Proximity Reader and Keypad, you cannot enroll by presenting to a reader. Follow the instructions for block enrollment in “Block Enrollment by Card Number Range” on page 3 of this section.***

NOTE: If you are using a mixed PXL/EntraGuard system where users need to be given both a card and a User ID, follow the instructions in “EntraGuard” on page 1 in section 10.

1. To enroll cards by presenting to a reader, click on the Setup ⇒ Users pull-down menu or click on the  tool bar button. These two icons  are added to the tool bar and the Setup Users spreadsheet window appears (see Figure 4-9). If the Setup Users spreadsheet window is not visible, click on the  tool bar button.

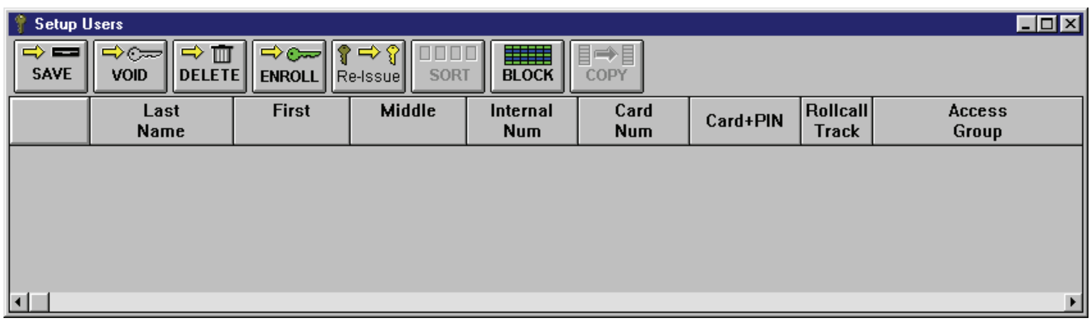


Figure 4-9: Setup Users Spreadsheet Window

2. Click on the  button. If the *Doors* program is not connected to the access control network, the program will automatically connect. The Enroll Cards window appears (see Figure 4-10).

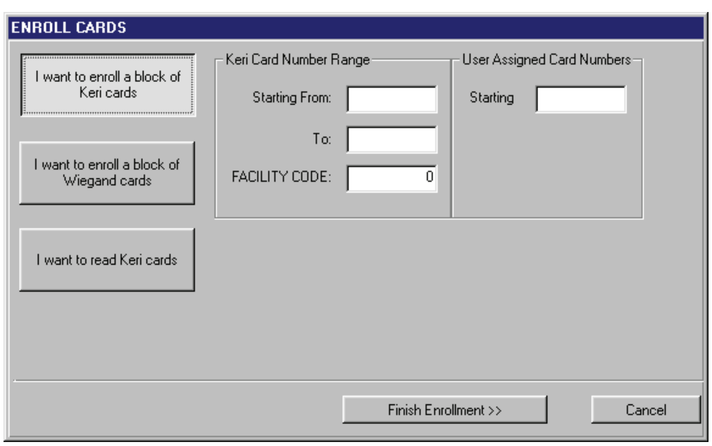


Figure 4-10: Enroll Cards Window

1.2.1 Enrolling Keri (Proximity) Cards by Presentation

1. For enrollment of Keri (Proximity) cards, click on the 

button. The Enroll Cards window changes for Keri card presentation (see Figure 4-11).

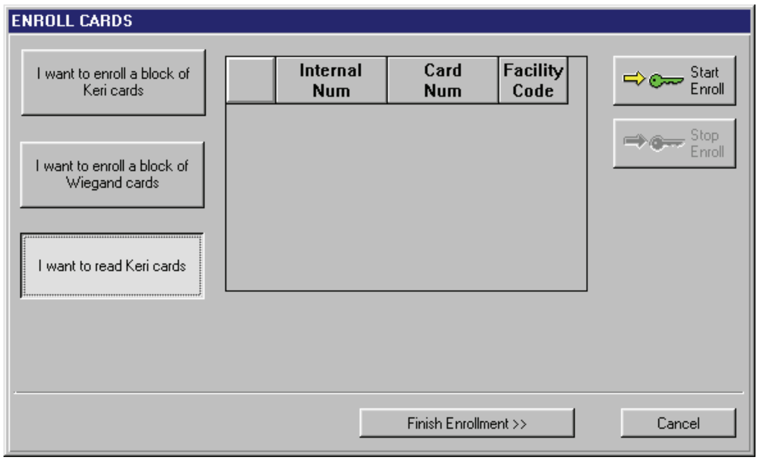


Figure 4-11: Enroll Cards Window for Presenting Keri Cards to a Reader

2. Click on the 

button. If the *Doors* program is not connected to the access control network, the program will automatically connect.
3. The "A" reader on the master controller is used for reading cards being enrolled. The reader's LED blinks green slowly to indicate it is ready for enrolling cards.

NOTE: The reader/controller is not available for any other use during the card enrollment process – any attempts to use a door associated with the master controller might disrupt the card enrollment process and will be denied until card enrollment is complete.

4. Skip to number 6 on page 10 of this section to continue the enrollment process.

1.2.2 Enrolling Wiegand Cards by Presentation

1. For enrollment of Wiegand cards by presenting to a reader, click on the 

. The Enroll Cards window changes for Wiegand card presentation (see Figure 4-12).

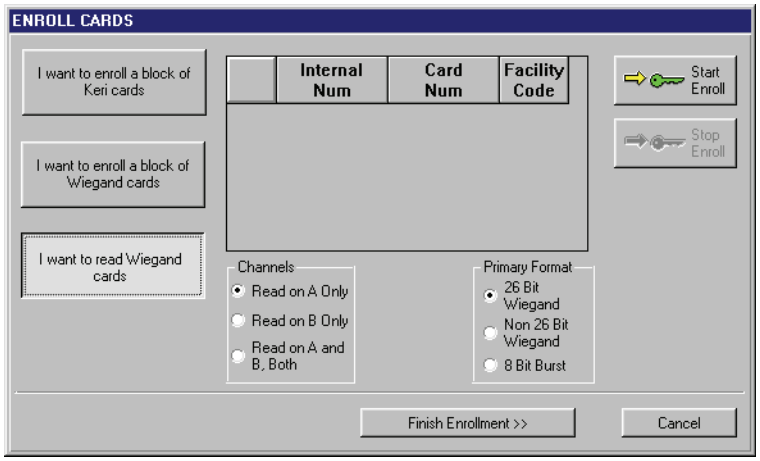


Figure 4-12: Enroll Cards Window for Presenting Wiegand Cards to a Reader

2. On a Wiegand master controller, the “A” reader, “B” reader, or both readers may be used for enrollment by presentation to a reader. In the “Channels” field, select which reader is to be used for enrollment by clicking on the corresponding radio button.
3. In the “Primary Format” field, select the kind of reader being used by clicking on the corresponding radio button.
4. Click on the 

button. If the *Doors* program is not connected to the access control network, the program will automatically connect.
5. The reader’s LED blinks green slowly to indicate it is ready for enrolling cards.

NOTE: The reader/controller is not available for any other use during the card enrollment process – any attempts to use a door associated with the master controller might disrupt the card enrollment process and will be denied until card enrollment is complete.

6. Present the first card to the enrollment reader. The reader will beep to indicate the card was read successfully and the card information will appear in the Enroll Cards window.

NOTE: If the Doors program is unable to enroll a card (because that card is faulty or has already been enrolled), the reader will provide one long beep and an error message window is displayed providing a brief description of the problem with the card being enrolled. Click the 

button to acknowledge the error message; then correct the problem and continue card enrollment. If there is no acknowledgement by the reader, after a card has been presented, the card may be of a format that is incompatible with the reader.

7. Present the second card to the enrollment reader. Again the reader will beep.
8. Continue presenting cards until all have been enrolled. When completed, the card enrollment window should look similar to Figure 4-13 on page 11 of this section.

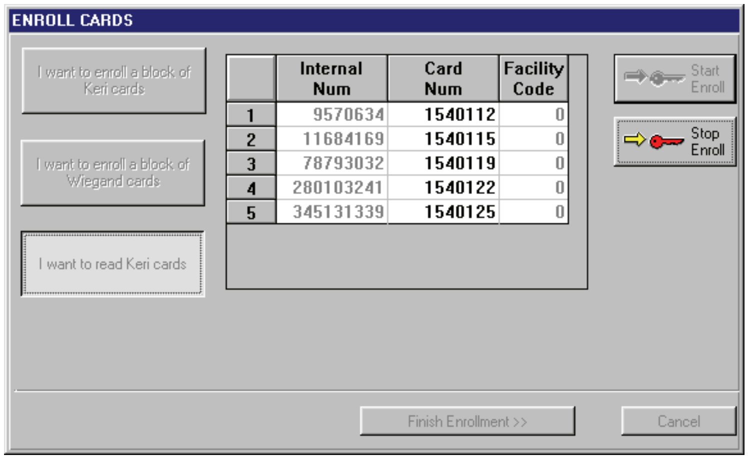
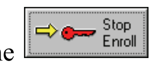


Figure 4-13: Enroll Cards Window for Presenting to a Reader – Cards Presented

9. Once all cards have been presented for enrollment, click on the  button to put the enrollment reader back into regular service.

10. Click on the  button. The Enroll New Users window displays a confirmation of enrollment (see Figure 4-14).

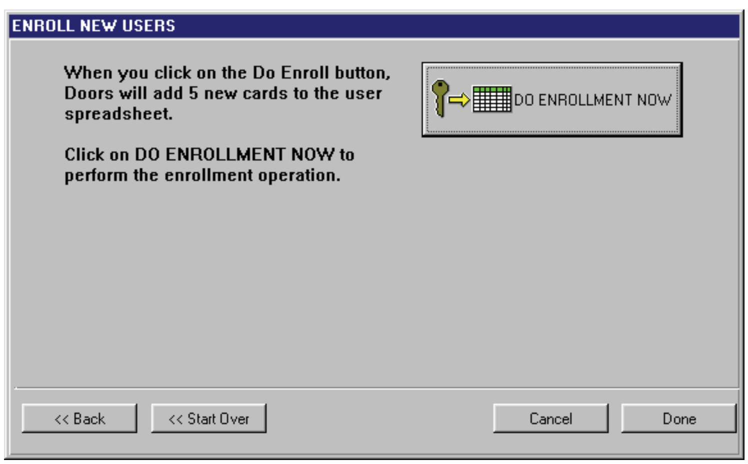
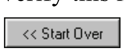
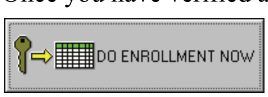


Figure 4-14: Enroll New Users Confirmation Window

11. The confirmation display shows the number of cards you are about to enroll. Take a moment to verify this number is correct. If this number is incorrect, click on the  button or the  button to return to the Enroll Cards window to make changes.

12. Once you have verified all the information is correct on the confirmation display, click on the  button. The cards are enrolled and the Enroll New Users window displays the enrollment results (see Figure 4-15 on page 12 of this section).

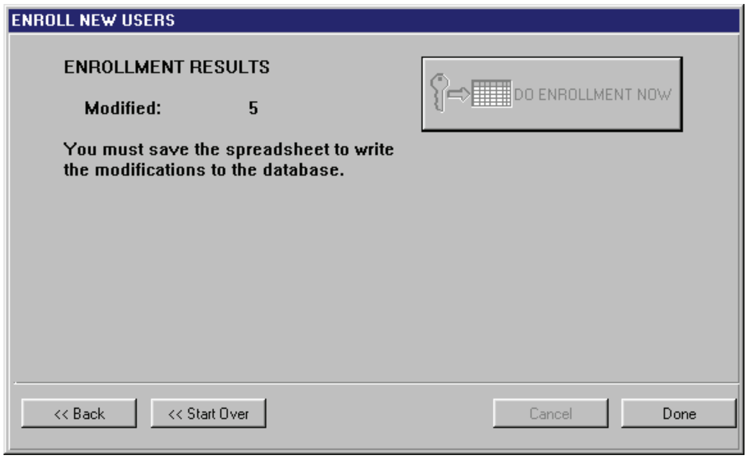


Figure 4-15: Enrollment Results Window

13. Carefully examine the information displayed under Enrollment Results. This field will alert you to the number of cards successfully enrolled and if there were any duplicates.
14. Click on the Done button to close the Enroll New Users window. The Setup Users spreadsheet window now contains the newly enrolled cards (see Figure 4-16).

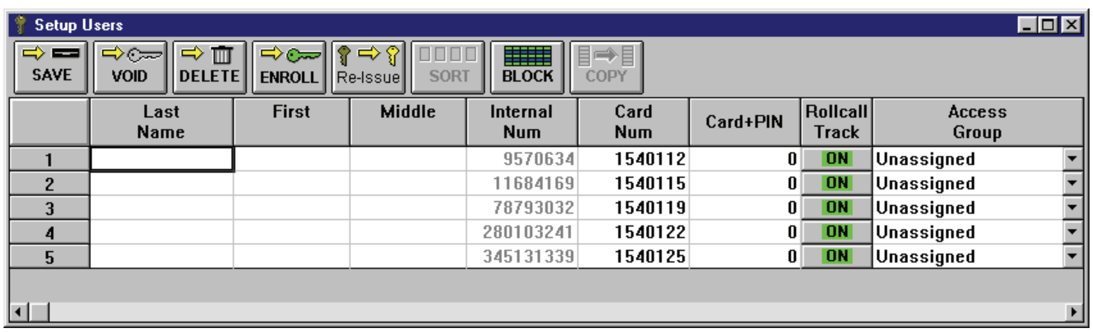


Figure 4-16: Setup Users Spreadsheet Window With Enrolled Presented Cards

15. Click on the SAVE button to save the enrollment. If the card enrollment information is not saved before clicking any other button or exiting the Setup Users window, the data entered is lost and must be re-entered.

2.0 Enter User Data

Once cards have been enrolled, user data may be entered by either the dialog box method or the spreadsheet method. Work with the method that feels the most comfortable to you.

2.1 User Data – Dialog Box Method

The dialog box method allows an operator to enter all user data through a series of "fill-in-the-blank" type windows. There are three data entry windows used to enter user information.

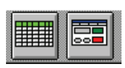
User Data – enter user data
Personal Setup – setup unique personal data entry fields
Preferences – enter card enrollment configuration preferences

NOTE: A fourth tab is automatically created when any personal fields are set up.

2.1.1 User Data Tab

The user data tab allows an operator to enter or edit personal data for each user database entry. It also allows an operator to void or delete a user. You must have enrolled cards before being able to enter user data (see "Card Enrollment" on page 3 of this section).

2.1.1.1 Entering User Data – Dialog Box Method

1. To enter user data, click on the Setup ⇒ Users pull-down menu or click on the  tool bar button. These two icons  are added to the tool bar and the Setup Users spreadsheet window appears.
2. Click on the  tool bar button to ensure the Setup Users dialog box window is active.
3. Click on the **User Data** tab. The User Data window appears (see Figure 4-17).

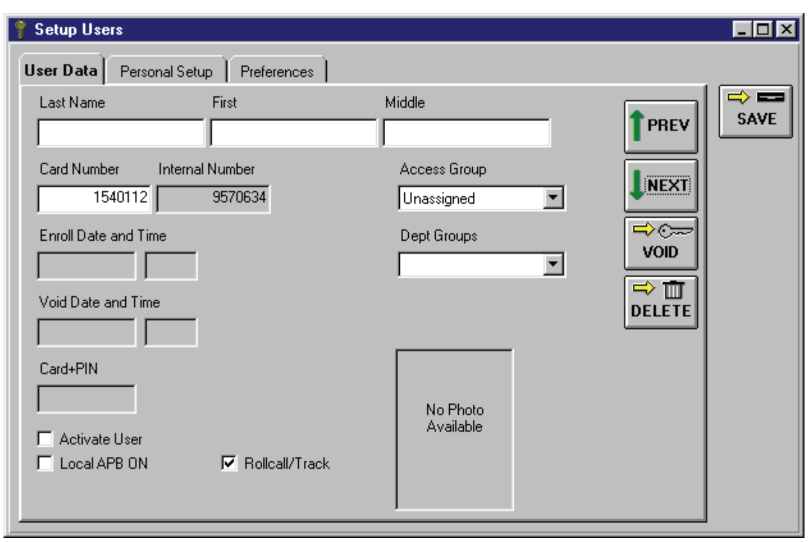


Figure 4-17: User Data Entry Window

4. Click on the 

buttons to scroll through the list of cards available and locate the card to which data should be entered.

NOTE: All block enrolled cards will have entries for both the internal number and card number. The internal number is the card's internal identification number – the number actually read from the card and processed by a reader. The card number is the number etched on the body of the card (entered during block enrollment). Cards enrolled by presenting to a reader may only have a value in the internal number field shown; if so, the card number field will be set to 0. The actual external number can be read from the body of the card and entered by an operator if desired.

NOTE: If you have block enrolled 26-bit Wiegand cards with the Card+PIN feature enabled, a card PIN is automatically generated at enrollment. That card PIN will be displayed in the Card+PIN field unless the operator has Read Only access to Setup Users. If an operator has Read Only access to Setup Users, this field will not appear even if a PIN is associated with the card.

5. Click in the **Last Name** field and enter the user's last name.
6. Click in the **First** name field and enter the user's first name.
7. Click in the **Middle** name field and enter the user's middle name or initial.
8. Locate the **Activate User** check box in the lower left corner of the User Data Entry window. Click in the box to activate the user. The date and time of the activation is entered as the Enroll Date and Time.
9. If the Card Number field displays a "0," the actual card number can be entered. Click in the **Card Number** field and type the card's number (the second set of digits printed on the body of the card, see Figure 4-3 on page 5 of this section).
10. Locate the **Local APB ON** check box. This check box enables/disables Local APB on individual users (see "Set Local Anti Passback" on page 13 in section 2). Click in the check box to enable anti passback checking for this user. To disable Local APB for this user, click in the check box and the check is removed.
11. Locate the **Rollcall/Track** check box. This enables/disables use of the Rollcall/Track feature with individual users (see "Set Rollcall/Track" on page 20 in section 2). Click in the check box to enable Rollcall/Track monitoring for this card. To disable Rollcall/Track for this user, click in the check box and the check is removed.

*NOTE: The **Local APB ON** and **Rollcall/Track** check boxes do not appear unless you have first enabled the features (see "Set Local Anti Passback" on page 13 in section 2 and "Set Rollcall/Track" on page 20 in section 2).*

12. Locate the **Access Group** field and select an access group to be assigned to this user. Click on the  and a list of the available access groups will appear. Click on the access group to be assigned to this user.
13. Locate the **Dept Groups** field and click on the  arrow. A list of existing department groups is displayed. Scroll through the list and if the desired department group name is in the list, click on that name. If the desired department group name does not exist, click in the **Dept Groups** field and type the name of the department group. Once a dept name has been entered, it is available for use with other users.

NOTE: A department group is a method of user identification based on the department for which a user works, i.e. Engineering, Janitorial, Management, Manufacturing, Sales, Stockroom. By using this field, user data can be sorted by department groups, displaying all members of a given group when in the Setup User spreadsheet view.

14. The resulting window should look similar to Figure 4-18.

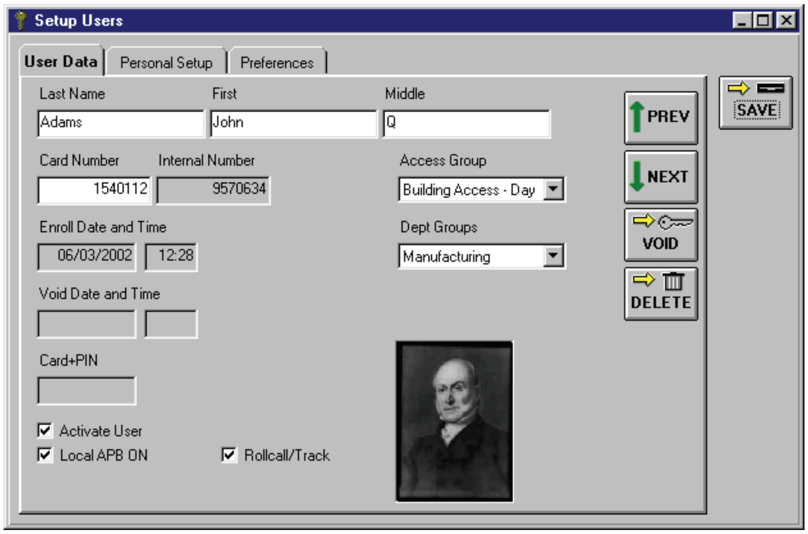


Figure 4-18: User Data Entry Window with User Information

15. Click on the  button. If the user data is not saved before clicking any other button or exiting the User Data window, the data entered is lost and must be re-entered.

NOTE: If you have enabled badging (see "Enable Badging in Doors" on page 15 in section 9), a photo window will appear in the lower right corner of the User Data window. Once a photo has been associated with the user (see "Acquire and Edit User Photo" on page 20 in section 9), that photo will show in the photo window (see Figure 4-18).

16. Now update the access control network with the new information. Click on the  button on the tool bar (for details on the update process refer to "Update the Network" on page 35 in section 5).

2.1.1.2 Editing User Data – Dialog Box Method

1. To edit user data, click on the Setup ⇒ Users pull-down menu or click on the tool bar button.

   These two icons are added to the tool bar and the Setup Users spreadsheet window appears.

2. Click on the tool bar button to ensure the setup users dialog box window is active.

3. Click on the **User Data** tab. Click on the buttons to scroll up and down the list of users and locate the user to be edited.
4. Edit the necessary fields.

5. Click on the button. If the edited user data is not saved before clicking any other button or exiting the User Data window, the data entered is lost and must be re-entered.

6. Now update the access control network with the new information. Click on the button on the tool bar (for details on the update process refer to "Update the Network" on page 35 in section 5).

NOTE: When edited user data is downloaded to the controllers, the counters keeping track of the APB amnesty value for the edited users are reset, allowing amnesty.

2.1.1.3 Voiding a User – Dialog Box Method

The void feature allows an operator to remove a user from the access control database without removing the card from the database. That card can then be reassigned to a new user while maintaining the history of who has held the card in the past.

1. To void a user, click on the Setup ⇒ Users pull-down menu or click on the tool bar button.

   These two icons are added to the tool bar and the Setup Users spreadsheet window appears.

2. Click on the tool bar button to ensure the setup users dialog box window is active.

3. Click on the **User Data** tab. Click on the buttons to scroll up and down the list of users and locate the user to be voided.

4. Click on the button. The current date and time is entered into the void date and time fields, and the user status is changed to inactive (the Activate User box is not checked).

5. Click on the button. If the voided user data is not saved before clicking any other button or exiting the User Data window, the void command is not applied to the database and must be redone.

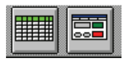
6. Now update the access control network with the new information. Click on the button on the tool bar (for details on the update process refer to "Update the Network" on page 35 in section 5).

2.1.1.4 Deleting a User – Dialog Box Method

The delete feature allows an operator to remove a card from the user database. A card that has been deleted from the user database must be re-enrolled if it is to be reused in the access control system.

NOTE: Although a deleted card is removed from the user database, it remains in the history and all events involving that card remain in the events data file. An event report can be performed, locating past events that involved any deleted card.

1. To delete a card, click on the Setup ⇒ Users pull-down menu or click on the  tool bar button.

   These two icons  are added to the tool bar and the Setup Users spreadsheet window appears.

2. Click on the  tool bar button to ensure the Setup Users dialog box window is active.
3. Click on the **User Data** tab. Click on the 

buttons to scroll through the list of users and locate the card to be deleted.
4. Before deleting a card, the user must be voided. If the user has not been voided, perform the void operation as described in “Voiding a User – Dialog Box Method” on page 16 of this section.
5. Once the user has been voided, click on the 

button. A deletion confirmation window appears (see Figure 4-19).

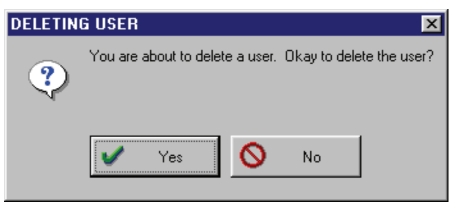
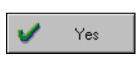


Figure 4-19: Deleting User Confirmation Window

6. Click on the 

button. The user entry in the database is now removed.
7. Click on the 

button. If the deleted data is not saved before clicking any other button or exiting the User Data window, the delete command is not applied to the database and must be redone.
8. Now update the access control network with the new information. Click on the 

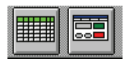
button on the tool bar (for details on the update process refer to “Update the Network” on page 35 in section 5).

2.1.2 Personal Data Fields Setup

The personal setup tab allows for the creation of up to six separate personal data categories to be designated for user data entry. Examples of fields that may be created are automobile license plate number, home telephone number, spouse's name, or other demographic information.

When a personal data category is created, a fourth tab, the Personal tab, will be added to the Setup Users dialog box window. The actual personal data for each user is entered in the personal tab.

2.1.2.1 Enable Personal Data Fields

1. To enable use of personal data fields, click on the Setup ⇒ Users pull-down menu or click on the  tool bar button. These two icons  are added to the tool bar and the Setup Users spreadsheet window appears.
2. Click on the  tool bar button to ensure the Setup Users dialog box window is active.
1. Click on the **Personal Setup** tab. The resulting window should look similar to Figure 4-20.

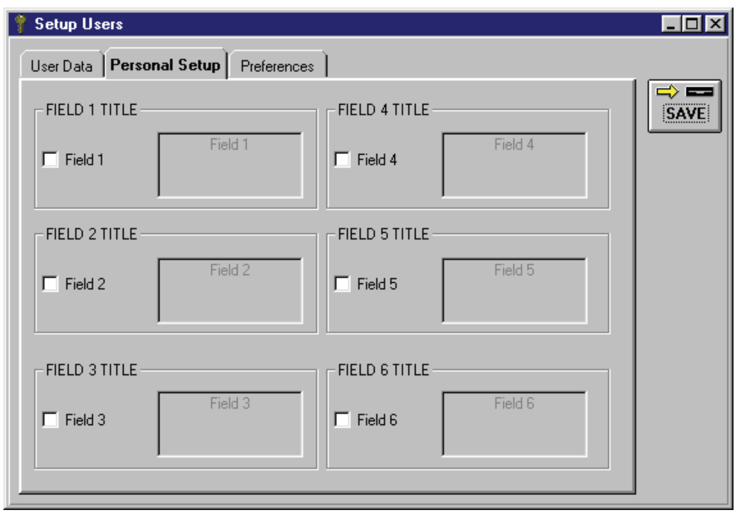


Figure 4-20: Personal Setup Tab

2. Click in the check box beside Field 1. A check mark will appear in the box, activating the field for assignment.
3. Click in the Field 1 assignment window. Use the backspace or delete keys on the keyboard to erase the "FIELD 1" text within the box.
4. Now type in the name to be designated to this field.
5. Click on the  button. If the personal data field changes are not saved before clicking any other button or exiting the Personal Setup window, the changes are lost and must be re-entered.
6. Once the Personal Setup tab has been saved, the Personal tab appears. The resulting window should look similar to Figure 4-21 on page 19 of this section.

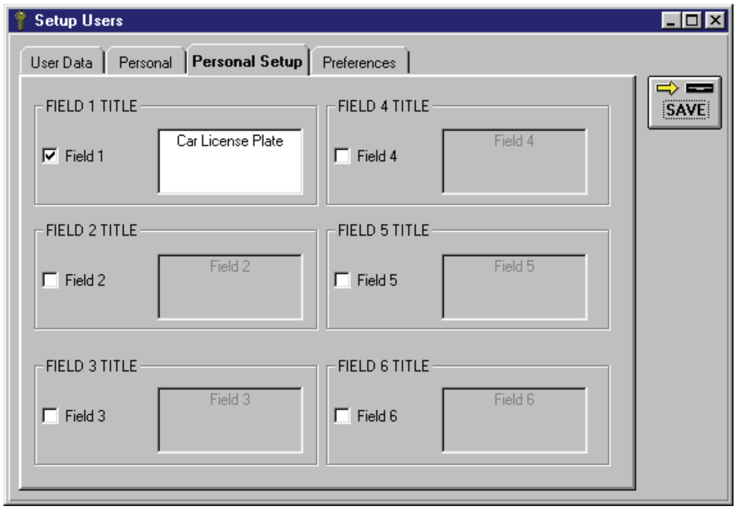
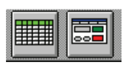


Figure 4-21: Personal Setup Tab - Field 1 Used

2.1.2.2 Enter Personal Data – Dialog Box Method

The Personal tab allows an operator to enter personal information regarding the user into the fields created in the Personal Setup tab. There is a 64 character maximum for each personal field.

1. To enter personal data for a user, click on the Setup ⇒ Users pull-down menu or click on the  tool bar button. These two icons  are added to the tool bar and the Setup Users spreadsheet window appears.
2. Click on the  tool bar button to ensure the Setup Users dialog box window is active.
3. Click on the **User Data** tab (if information for a user has been previously entered it will be visible in the window).
4. Click on the  buttons to scroll through the list of users and locate the one to which personal data should be entered.

5. Click on the **Personal** tab. All personal fields that were setup previously will be available for information to be typed in.
6. Click in the personal field to be used and enter the appropriate information. The resulting window should look similar to Figure 4-22 on page 20 of this section.

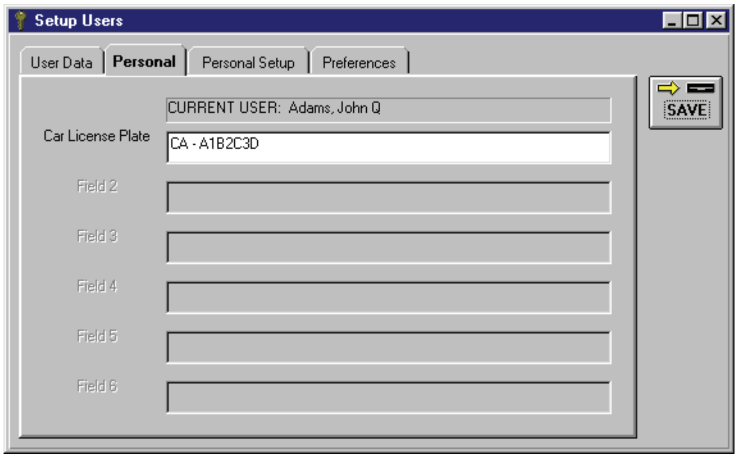


Figure 4-22: Personal Tab

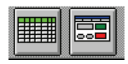
7. Click on the 

button. If the personal data entries are not saved before clicking any other button or exiting the Personal data window, the changes are lost and must be re-entered.

2.1.3 Preferences Tab

The preferences tab allows an operator to set user data display information. Certain features might not be needed for your system. To prevent displaying unnecessary information, these features can be disabled. The default is for all of these features to be disabled. The following features can be disabled.

- internal card numbers
- card formats
- card numbers
- facility codes
- department groups
- EntraGuard IDs

1. To change a preference for the user database, click on the Setup ⇒ Users pull-down menu or click on the  tool bar button. These two icons  are added to the tool bar and the Setup Users spreadsheet window appears.
2. Click on the  tool bar button to ensure the setup users dialog box window is active.
3. Click on the **Preferences** tab. The resulting window should look similar to Figure 4-23.

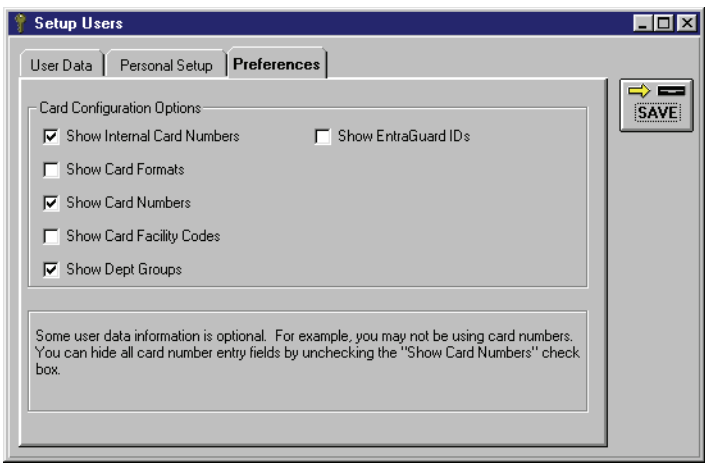
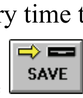


Figure 4-23: Preferences Tab

4. If the box beside the preference option has a check mark, the option is enabled; if there is not a check mark, the option is disabled. To change a preference option, click on the box beside the option. Every time the box is clicked, it changes state between on and off.
5. Click on the  button. If the preference options are not saved before clicking any other button or exiting the Preferences window, the preference options are lost and must be re-entered.

2.2 User Data – Spreadsheet Method

The spreadsheet method allows an operator to enter user data directly into a spreadsheet. It also allows an operator to void a user or delete a card. The spreadsheet creates a row for each enrolled user, and has database columns for every parameter.

NOTE: The generic term "card" also applies to Keri Systems' PKT-10 key tags. Any operational differences between proximity cards and key tags will be identified as applicable.

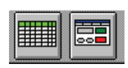
2.2.1 Entering User Data – Spreadsheet Method

User data can be entered for all users displayed in the spreadsheet window. Newly enrolled cards display an internal card number (and may display a card number), but have blank cells or default values for all other spreadsheet entries in that user's row.

NOTE: Fields enabled or disabled in the Preferences tab dialog box also apply to the spreadsheet. Make sure you have selected all the fields that must be shown (see "Preferences Tab" on page 21 of this section).

Once cards have been enrolled (see "Card Enrollment" on page 3 of this section), data can be entered or edited for all users displayed in the spreadsheet.

NOTE: Additional columns that appear when the EntraGuard feature has been enabled are described in "EntraGuard" on page 1 in section 10.

1. To enter user data through the spreadsheet method, click on the Setup ⇒ Users pull-down menu or click on the  tool bar button. These two icons  are added to the tool bar and the Setup Users spreadsheet window appears (see Figure 4-24). If the Setup Users spreadsheet window is not visible, click on the  tool bar button.

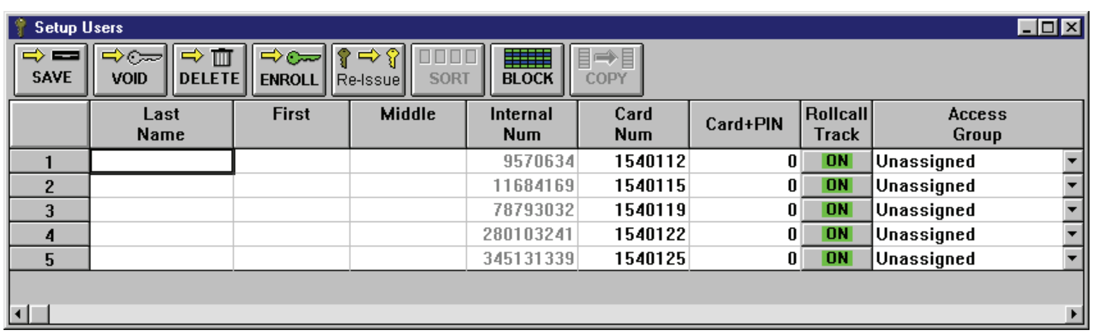


Figure 4-24: Setup Users Spreadsheet Window with Enrolled Cards

Last Name
The user's last name is entered in this cell. Click in the cell and enter the user's last name.

First
The user's first name is entered in this cell. Click in the cell and enter the user's first name.

Middle
The user's middle name or initial is entered in this cell. Click in the cell and enter the user's middle name or initial.

Internal Number

The internal number value is automatically entered when a card is enrolled. It is the card's internal identification number, read from the card when the card was presented to the enrollment reader. This field cannot be edited.

Card Number

The card number refers to the number printed onto the body of the card (see Figure 4-25). The card number is the second set of digits printed on the body of the card (in Figure 4-25, it is the digits corresponding to 187491). The card number will be longer than 4 digits. For this example, the entire number of this card is K1757 187491; the card number is 187491, 6 digits long.

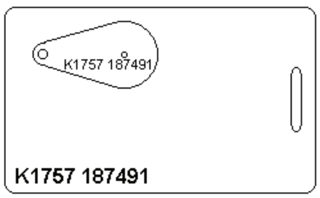


Figure 4-25: Proximity Card Number

NOTE: The Card Number is an optional field. A card number is not automatically entered and is not required for program operation.

Card+PIN

If you are using the P-650 Card+PIN Proximity Reader and Keypad, and have enabled the Card+PIN option (see "Set Card+PIN (P-650) Mode" on page 22 in section 2), the card PIN (Personal Identification Number) is automatically generated and assigned to a card during block enrollment. The PIN cannot be changed or edited. The Card+PIN will not be visible if the operator has been assigned Read Only rights for Setup Users (see "Setup Operators" on page 45 in section 2).

NOTE: Due to the algorithm used in generating a card PIN, it is possible for cards to have the same PIN. Most card access systems allow for duplicate PINs associated with different cards. PIN duplication does not compromise the security of the system.

Rollcall/Track

The Rollcall/Track cell selects a user to appear in the Rollcall/Track monitoring window (see "Set Rollcall/Track" on page 20 in section 2). If you have enabled the Rollcall/Track option under Setup System, the Rollcall/Track cell option default is ON during enrollment.

1. To **inactivate** Rollcall/Track, locate the On/Off cell. It should be 

.
2. Click on the cell; it changes to 

.
3. To **activate** Rollcall/Track, locate the On/Off cell. It should be 

.
4. Click on the cell; it changes to 

.

NOTE: The Rollcall/Track column does not appear unless you have enabled the Rollcall/Track option (see "Set Rollcall/Track" on page 20 in section 2).

Access Group

An access group must be assigned to each user. The access group defines through which doors and at what time-of-the-day and day-of-the-week an individual user will be granted access.

1. Locate the Access Group cell. Click on the and a list of the available access groups appears. Scroll through this list and find the access group to be assigned to the user.

Based on entries made so far, the Setup Users spreadsheet should look similar to Figure 4-26.

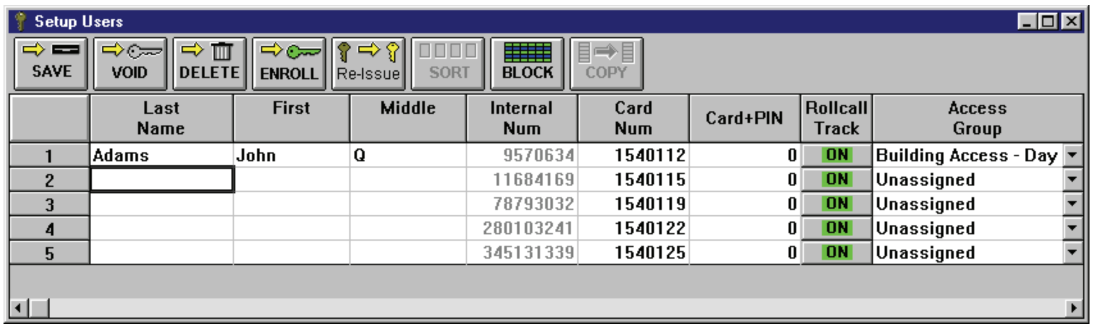


Figure 4-26: Setup Users Spreadsheet With Enrolled User – Part 1

Depending upon the size and resolution of the computer's screen, more of the spreadsheet may be displayed than is shown in Figure 4-26. If any portion of the spreadsheet is not displayed a scroll bar appears across the bottom of the spreadsheet. For the following spreadsheet column descriptions, ensure all the columns to the right of the access group column are displayed by clicking on until the last column appears (this should be the Void Time column unless you have set up any Personal fields in the "Personal Data Fields Setup" on page 18 of this section).

Department Group

A department group is a method of user identification based on the department for which a user works, i.e. Engineering, Janitorial, Management, Manufacturing, Sales, Stockroom. By using this field, user data can be sorted by department groups, displaying all members of a given group. Instructions for sorting data is provided in "Sorting Data" on page 29 of this section.

1. Locate the Department Group cell. Click on the and a list of the available department groups appears. Scroll through this list and find the department group to be assigned to this user.
2. If an appropriate department group can be found, click on the **Department Group** name.
3. If an appropriate department group cannot be found, a new one can be entered. Double-click in the **Department Group** cell and type the department group name you want to use.
4. Click on the SAVE button. If the department group name is not saved before clicking any other button or exiting the Setup Users Spreadsheet window, the department group is lost and must be re-entered.

On/Off

The On/Off cell makes a user active or inactive. When a user is first enrolled, the user is inactive and must be activated to be read by readers.

You may inactivate a user when the user goes on vacation or takes a leave-of-absence and should not have access during this period. This can prevent an unauthorized person from using their card to gain access to a secured area. When the user is due to return, activate the user and access will be granted again.

1. To **activate** a user, locate the On/Off cell. It should be .
2. Click on the cell; it changes to .
3. To **inactivate** a user, locate the On/Off cell. It should be .
4. Click on the cell; it changes to .

Local APB

The Local APB cell enables the anti passback feature for a user. When a user is first enrolled, the local APB is inactive. Local APB must be made active to be applied to users by controllers. For more information on Local APB, see “Set Local Anti Passback” on page 13 in section 2.

1. To **activate** Local APB, locate the On/Off cell. It should be .
2. Click on the cell; it changes to .
3. To **inactivate** Local APB, locate the On/Off cell. It should be .
4. Click on the cell; it changes to .

NOTE: The Local APB column does not appear unless you have activated the Local APB option (see “Set Local Anti Passback” on page 13 in section 2).

Enroll Date and Time

When a user is activated for the first time, the date and time of activation is automatically entered into the Enroll Date and Enroll Time cells of the spreadsheet. These cells are not editable.

Void Date and Time

When a user is voided, the date and time is automatically entered into the Void Date and Void Time cells of the spreadsheet. These cells are not editable.

Personal Fields

An operator can assign up to six personal data fields which are added to the Setup Users spreadsheet. These data fields are used for information such as an automobile license plate, home telephone number, spouse’s name, demographic information. For information on creating a personal data field, see “Personal Data Fields Setup” on page 18 of this section.

1. Once personal fields have been created, click on the applicable cell and type the necessary information.

Based on the last set of entries and the Personal Data Fields section previously discussed, the second half of the cards spreadsheet should look similar to Figure 4-27 on page 26 of this section.

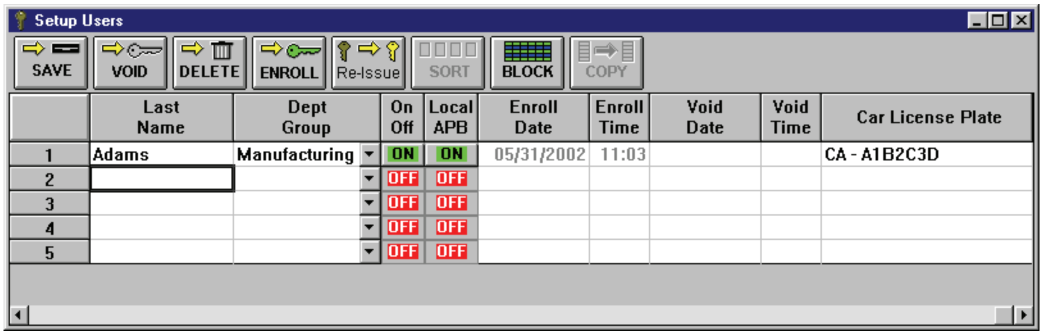


Figure 4-27: Setup Users Spreadsheet With Enrolled User – Part 2

2. Once all information is entered, click on the 

button. If the user data is not saved before clicking any other button or exiting the Setup Users spreadsheet window, the changes are lost and must be re-entered.

3. Now update the access control network with the new information. Click on the 

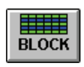
button on the tool bar (for details on the update process refer to “Update the Network” on page 35 in section 5).

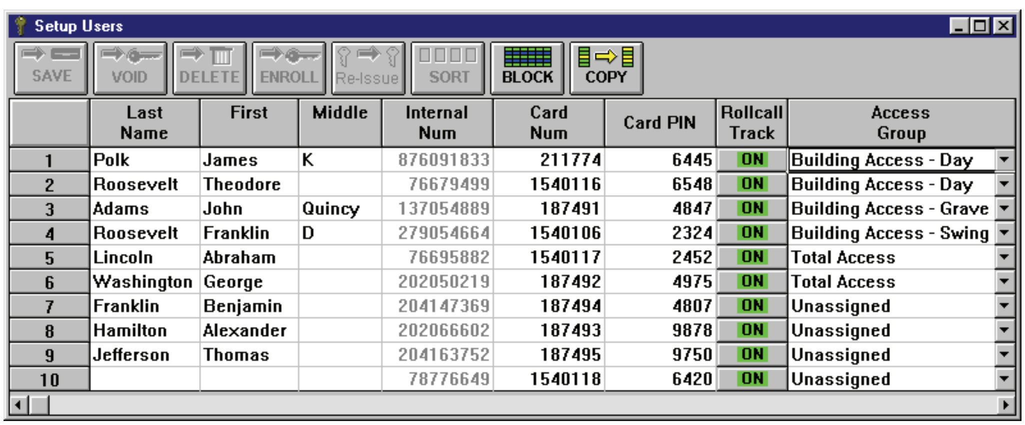
2.2.2 Block Copying Data

The Block and Copy buttons allow an operator to select a data cell for copying to other data cells. This can be helpful when enrolling a large number of users where a set of cells will all have the same information. For example, when enrolling a group of users assigned the day shift, the access and department groups for the entire group might be the same. To minimize data entry, enter the information for the first user and then copy it to the remaining users. The following fields can be block copied.

- Card Num
- Rollcall/Track
- Access Group
- Dept Group
- On/Off
- Local APB
- Personal Data

An example will be shown where the access group will be copied from one day shift user to three new day shift users.

1. Click on the cell from which data should be copied.
2. Click on the  button (see Figure 4-28).

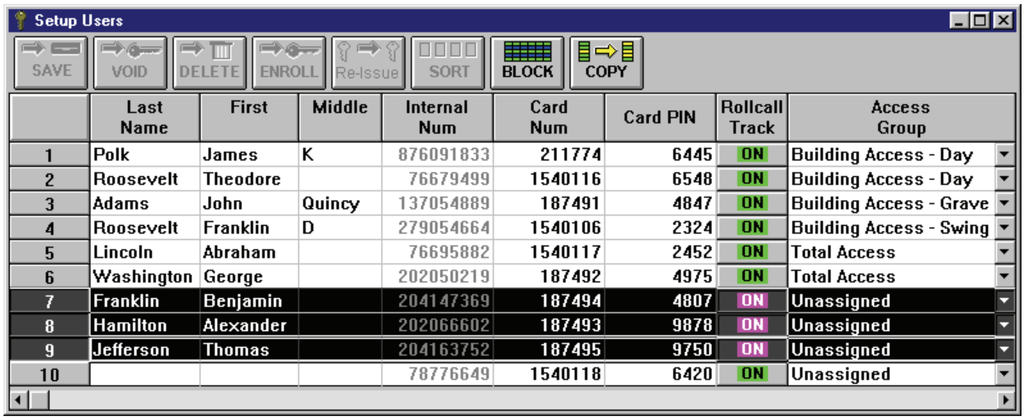


	Last Name	First	Middle	Internal Num	Card Num	Card PIN	Rollcall Track	Access Group
1	Polk	James	K	876091833	211774	6445	ON	Building Access - Day
2	Roosevelt	Theodore		76679499	1540116	6548	ON	Building Access - Day
3	Adams	John	Quincy	137054889	187491	4847	ON	Building Access - Grave
4	Roosevelt	Franklin	D	279054664	1540106	2324	ON	Building Access - Swing
5	Lincoln	Abraham		76695882	1540117	2452	ON	Total Access
6	Washington	George		202050219	187492	4975	ON	Total Access
7	Franklin	Benjamin		204147369	187494	4807	ON	Unassigned
8	Hamilton	Alexander		202066602	187493	9878	ON	Unassigned
9	Jefferson	Thomas		204163752	187495	9750	ON	Unassigned
10				78776649	1540118	6420	ON	Unassigned

Figure 4-28: Block Selected Data Ready for Copying

3. There are three ways to block select the cells to which data is copied. Use the method you find easiest.

- Click and hold on the first cell to copy and then drag the mouse down to the last cell to copy.
- Click on the first cell, hold the Shift key down, and click on the last cell (see Figure 4-29 on page 28 of this section).
- Hold the Ctrl key down and one-at-a-time click on the cells to be copied. This method is best used when receiving cells are not in sequential order.

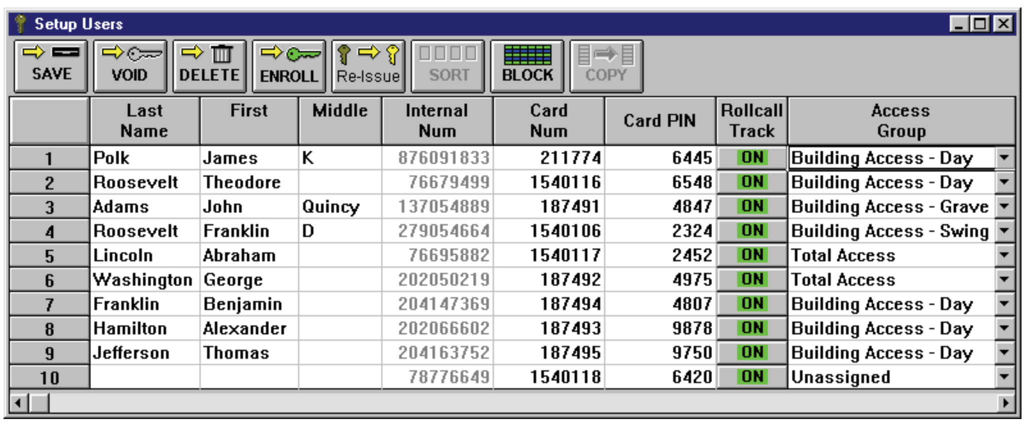


	Last Name	First	Middle	Internal Num	Card Num	Card PIN	Rollcall Track	Access Group
1	Polk	James	K	876091833	211774	6445	ON	Building Access - Day
2	Roosevelt	Theodore		76679499	1540116	6548	ON	Building Access - Day
3	Adams	John	Quincy	137054889	187491	4847	ON	Building Access - Grave
4	Roosevelt	Franklin	D	279054664	1540106	2324	ON	Building Access - Swing
5	Lincoln	Abraham		76695882	1540117	2452	ON	Total Access
6	Washington	George		202050219	187492	4975	ON	Total Access
7	Franklin	Benjamin		204147369	187494	4807	ON	Unassigned
8	Hamilton	Alexander		202066602	187493	9878	ON	Unassigned
9	Jefferson	Thomas		204163752	187495	9750	ON	Unassigned
10				78776649	1540118	6420	ON	Unassigned

Figure 4-29: Copy Data Rows Selected

4. Click on the 

button. All copyable data will be transferred (see Figure 4-30).



	Last Name	First	Middle	Internal Num	Card Num	Card PIN	Rollcall Track	Access Group
1	Polk	James	K	876091833	211774	6445	ON	Building Access - Day
2	Roosevelt	Theodore		76679499	1540116	6548	ON	Building Access - Day
3	Adams	John	Quincy	137054889	187491	4847	ON	Building Access - Grave
4	Roosevelt	Franklin	D	279054664	1540106	2324	ON	Building Access - Swing
5	Lincoln	Abraham		76695882	1540117	2452	ON	Total Access
6	Washington	George		202050219	187492	4975	ON	Total Access
7	Franklin	Benjamin		204147369	187494	4807	ON	Building Access - Day
8	Hamilton	Alexander		202066602	187493	9878	ON	Building Access - Day
9	Jefferson	Thomas		204163752	187495	9750	ON	Building Access - Day
10				78776649	1540118	6420	ON	Unassigned

Figure 4-30: Data Copied

5. Click on the 

button. If the copied data is not saved before clicking any other button or exiting the Setup Users spreadsheet window, the changes are lost and must be re-entered.

6. Now update the access control network with the new information. Click on the 

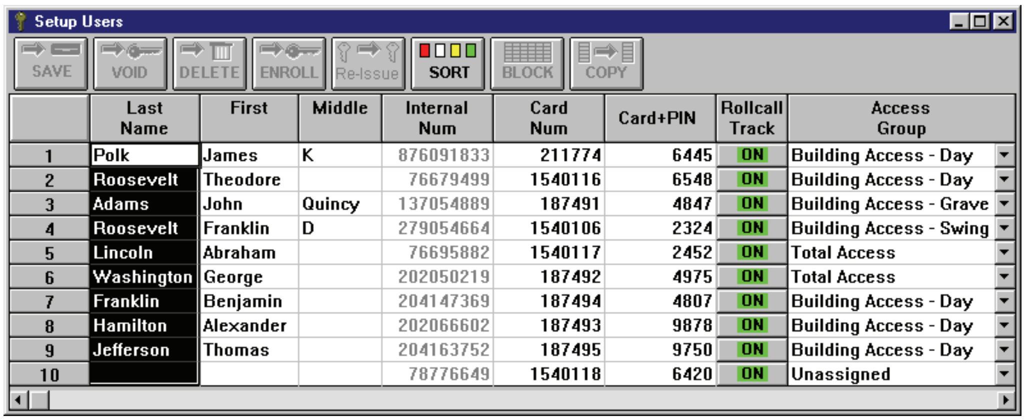
button on the tool bar (for details on the update process refer to "Update the Network" on page 35 in section 5).

2.2.3 Sorting Data

The sort data button allows an operator to display the data in the spreadsheet in a desired order (always from A to Z or from lowest to highest number). For example, sorting by last name places all users in alphabetical, last name order. Sorting by department group places all users in alphabetical department group order. Sorting by card number places all users in numeric card number order. Sorting by void date places all users in void date order followed by the users that are not voided. Keri Systems recommends sorting the data in the spreadsheet so that information is grouped in a manner that makes it easy to find desired information.

All of the spreadsheet fields can be sorted.

1. Click on the top of the column you want to sort by. The entire column is highlighted (see Figure 4-31).

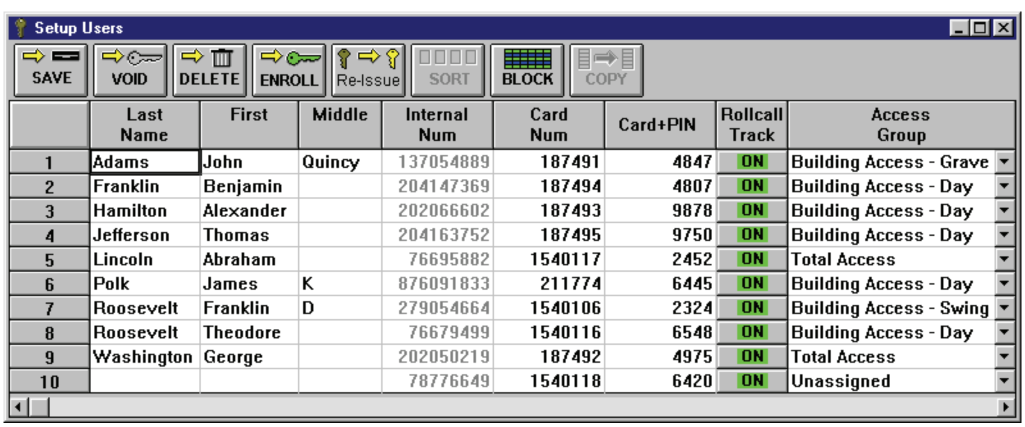


	Last Name	First	Middle	Internal Num	Card Num	Card+PIN	Rollcall Track	Access Group
1	Polk	James	K	876091833	211774	6445	ON	Building Access - Day
2	Roosevelt	Theodore		76679499	1540116	6548	ON	Building Access - Day
3	Adams	John	Quincy	137054889	187491	4847	ON	Building Access - Grave
4	Roosevelt	Franklin	D	279054664	1540106	2324	ON	Building Access - Swing
5	Lincoln	Abraham		76695882	1540117	2452	ON	Total Access
6	Washington	George		202050219	187492	4975	ON	Total Access
7	Franklin	Benjamin		204147369	187494	4807	ON	Building Access - Day
8	Hamilton	Alexander		202066602	187493	9878	ON	Building Access - Day
9	Jefferson	Thomas		204163752	187495	9750	ON	Building Access - Day
10				78776649	1540118	6420	ON	Unassigned

Figure 4-31: Preparing to Sort User Data

2. Click on the 

button. All data in the spreadsheet is reorganized into alphabetical order by last name (see Figure 4-32).



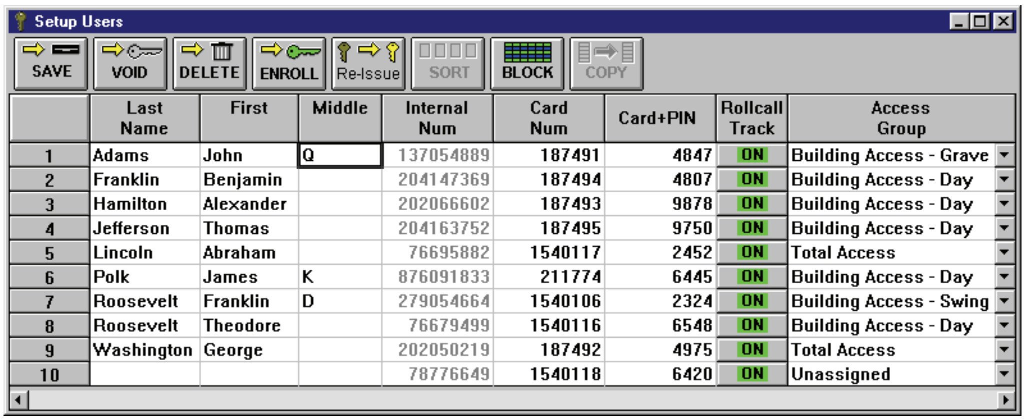
	Last Name	First	Middle	Internal Num	Card Num	Card+PIN	Rollcall Track	Access Group
1	Adams	John	Quincy	137054889	187491	4847	ON	Building Access - Grave
2	Franklin	Benjamin		204147369	187494	4807	ON	Building Access - Day
3	Hamilton	Alexander		202066602	187493	9878	ON	Building Access - Day
4	Jefferson	Thomas		204163752	187495	9750	ON	Building Access - Day
5	Lincoln	Abraham		76695882	1540117	2452	ON	Total Access
6	Polk	James	K	876091833	211774	6445	ON	Building Access - Day
7	Roosevelt	Franklin	D	279054664	1540106	2324	ON	Building Access - Swing
8	Roosevelt	Theodore		76679499	1540116	6548	ON	Building Access - Day
9	Washington	George		202050219	187492	4975	ON	Total Access
10				78776649	1540118	6420	ON	Unassigned

Figure 4-32: Sorted User Data

2.2.4 Editing User Data – Dialog Box Method

Editing user data is simply a matter of locating the cell requiring editing and entering the new information.

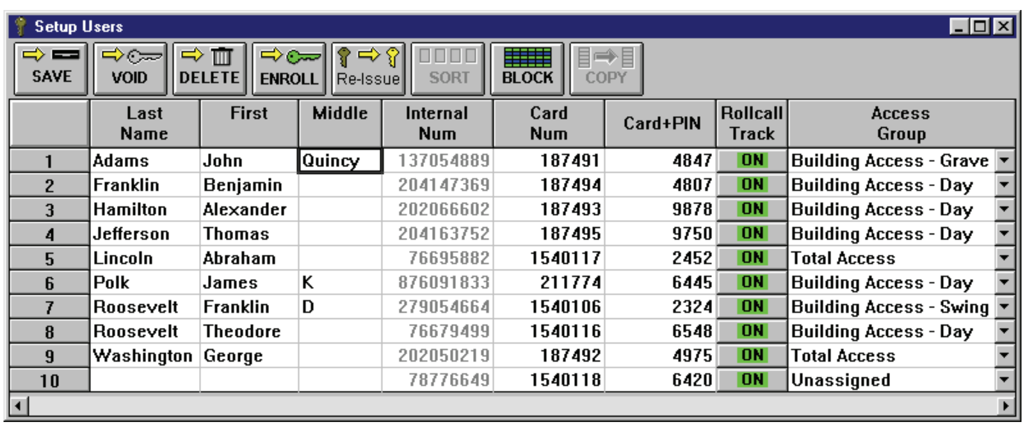
1. Locate the user for which an edit needs to be made in the spreadsheet.
2. If necessary, use the scroll bar and scroll left and right across the spreadsheet to locate the cell where the edit will take place.
3. Click on the cell (see Figure 4-33).



	Last Name	First	Middle	Internal Num	Card Num	Card+PIN	Rollcall Track	Access Group
1	Adams	John	Q	137054889	187491	4847	ON	Building Access - Grave
2	Franklin	Benjamin		204147369	187494	4807	ON	Building Access - Day
3	Hamilton	Alexander		202066602	187493	9878	ON	Building Access - Day
4	Jefferson	Thomas		204163752	187495	9750	ON	Building Access - Day
5	Lincoln	Abraham		76695882	1540117	2452	ON	Total Access
6	Polk	James	K	876091833	211774	6445	ON	Building Access - Day
7	Roosevelt	Franklin	D	279054664	1540106	2324	ON	Building Access - Swing
8	Roosevelt	Theodore		76679499	1540116	6548	ON	Building Access - Day
9	Washington	George		202050219	187492	4975	ON	Total Access
10				78776649	1540118	6420	ON	Unassigned

Figure 4-33: Select a Cell to Edit

4. As you enter the new information, it overwrites the existing information (see Figure 4-34).



	Last Name	First	Middle	Internal Num	Card Num	Card+PIN	Rollcall Track	Access Group
1	Adams	John	Quincy	137054889	187491	4847	ON	Building Access - Grave
2	Franklin	Benjamin		204147369	187494	4807	ON	Building Access - Day
3	Hamilton	Alexander		202066602	187493	9878	ON	Building Access - Day
4	Jefferson	Thomas		204163752	187495	9750	ON	Building Access - Day
5	Lincoln	Abraham		76695882	1540117	2452	ON	Total Access
6	Polk	James	K	876091833	211774	6445	ON	Building Access - Day
7	Roosevelt	Franklin	D	279054664	1540106	2324	ON	Building Access - Swing
8	Roosevelt	Theodore		76679499	1540116	6548	ON	Building Access - Day
9	Washington	George		202050219	187492	4975	ON	Total Access
10				78776649	1540118	6420	ON	Unassigned

Figure 4-34: Edited Cell

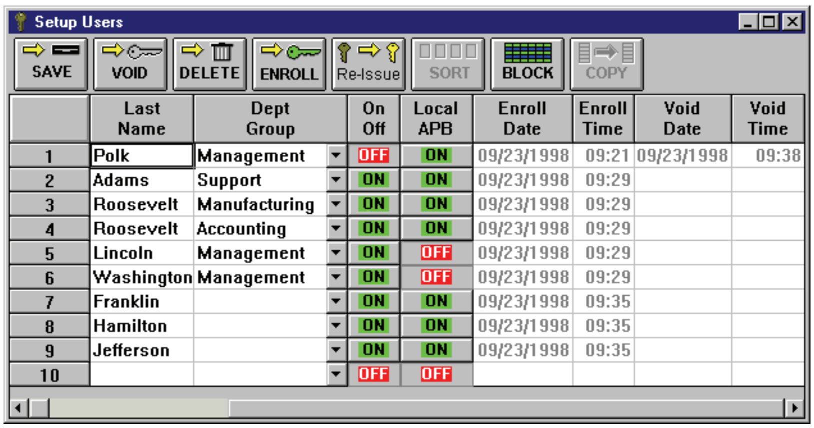
5. Click on the  button. If the edited cell data is not saved before clicking any other button or exiting the Setup Users spreadsheet window, the changes are lost and must be re-entered.

2.2.5 Voiding a User – Dialog Box Method

The void users feature allows an operator to remove a user from the access control database without removing the card from the database. That card can then be reassigned to a new user while maintaining the history of who has held the card in the past.

1. Scroll up and down the list of available users and locate the user who will be voided.
2. Click on the **Last Name** cell, or any cell on that user row (see Figure 4-35).
3. Click on the 

button. The user is inactivated and the void date and time is entered into the spreadsheet (see Figure 4-35). This card will not be accepted by any reader/controller in the access control system.



	Last Name	Dept Group	On Off	Local APB	Enroll Date	Enroll Time	Void Date	Void Time
1	Polk	Management	OFF	ON	09/23/1998	09:21	09/23/1998	09:38
2	Adams	Support	ON	ON	09/23/1998	09:29		
3	Roosevelt	Manufacturing	ON	ON	09/23/1998	09:29		
4	Roosevelt	Accounting	ON	ON	09/23/1998	09:29		
5	Lincoln	Management	ON	OFF	09/23/1998	09:29		
6	Washington	Management	ON	OFF	09/23/1998	09:29		
7	Franklin		ON	ON	09/23/1998	09:35		
8	Hamilton		ON	ON	09/23/1998	09:35		
9	Jefferson		ON	ON	09/23/1998	09:35		
10			OFF	OFF				

Figure 4-35: Voided User

4. Click on the 

button. If the voided user is not saved before clicking any other button or exiting the Setup Users spreadsheet window, the changes are lost and must be re-entered.

5. Now update the access control network with the new information. Click on the 

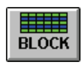
button on the tool bar (for details on the update process refer to “Update the Network” on page 35 in section 5).

2.2.6 Block Voiding Users

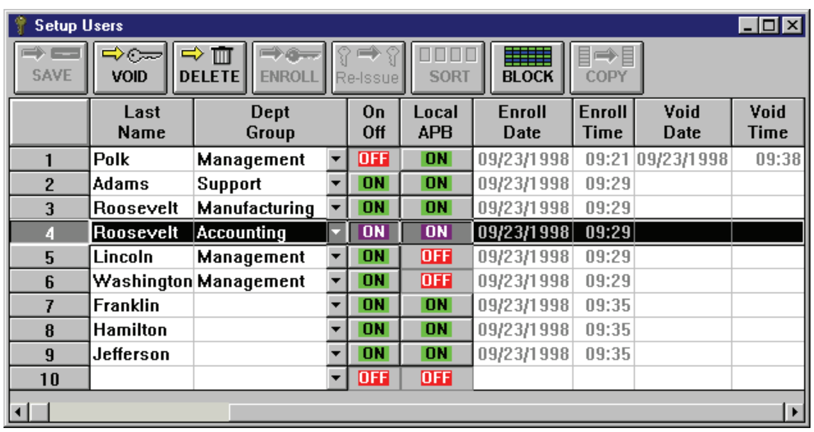
The Block and Void buttons allow an operator to select a number of users to be voided all at one time, removing the users from the access control database without removing the cards from the database. Cards can then be reassigned to new users while maintaining the history of those who held the cards in the past.

1. Click on one of the following cells from the first user row to be voided.

- Last Name
- First
- Middle
- Enroll Date
- Enroll Time
- Void Date
- Void Time

2. Click on the 

button (see Figure 4-36).

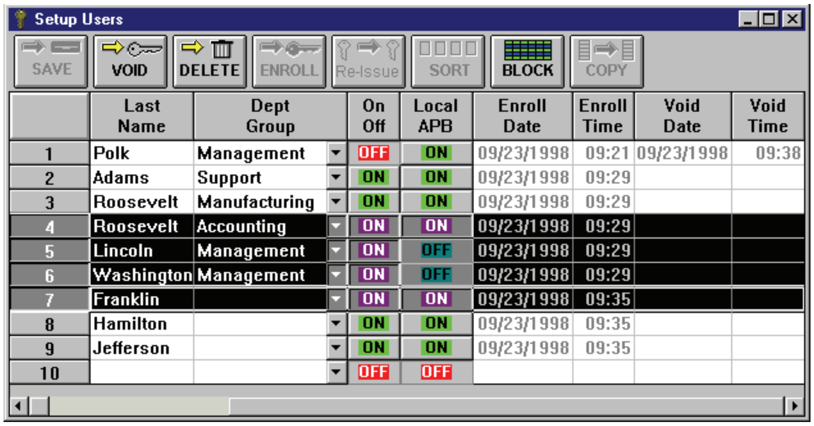


	Last Name	Dept Group	On Off	Local APB	Enroll Date	Enroll Time	Void Date	Void Time
1	Polk	Management	OFF	ON	09/23/1998	09:21	09/23/1998	09:38
2	Adams	Support	ON	ON	09/23/1998	09:29		
3	Roosevelt	Manufacturing	ON	ON	09/23/1998	09:29		
4	Roosevelt	Accounting	ON	ON	09/23/1998	09:29		
5	Lincoln	Management	ON	OFF	09/23/1998	09:29		
6	Washington	Management	ON	OFF	09/23/1998	09:29		
7	Franklin		ON	ON	09/23/1998	09:35		
8	Hamilton		ON	ON	09/23/1998	09:35		
9	Jefferson		ON	ON	09/23/1998	09:35		
10			OFF	OFF				

Figure 4-36: Select the First Block Void User

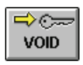
3. There are three ways to block select the users to be voided. Use the method you find easiest.

- Click and hold on the first cell to copy and then drag the mouse down to the last user to void.
- Click on the first cell, hold the Shift key down, and click on the last user to void (see Figure 4-37 on page 33 of this section).
- Hold the Ctrl key down and one-at-a-time click on the users to be voided. This method is best used when users are not in sequential order.

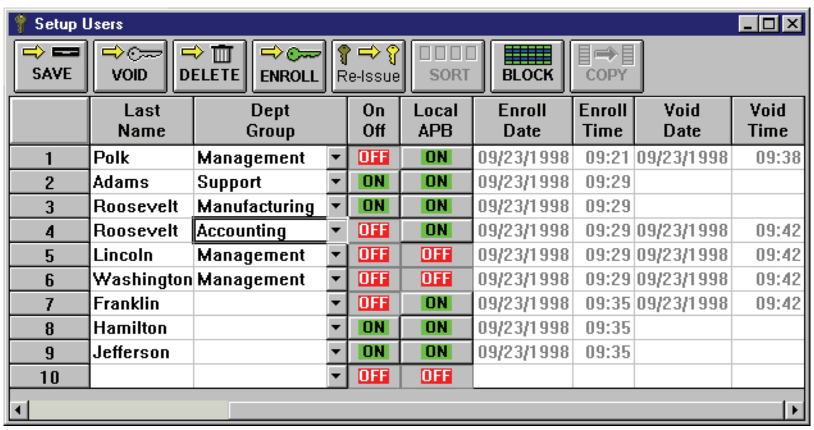


	Last Name	Dept Group	On Off	Local APB	Enroll Date	Enroll Time	Void Date	Void Time
1	Polk	Management	OFF	ON	09/23/1998	09:21	09/23/1998	09:38
2	Adams	Support	ON	ON	09/23/1998	09:29		
3	Roosevelt	Manufacturing	ON	ON	09/23/1998	09:29		
4	Roosevelt	Accounting	ON	ON	09/23/1998	09:29		
5	Lincoln	Management	ON	OFF	09/23/1998	09:29		
6	Washington	Management	ON	OFF	09/23/1998	09:29		
7	Franklin		ON	ON	09/23/1998	09:35		
8	Hamilton		ON	ON	09/23/1998	09:35		
9	Jefferson		ON	ON	09/23/1998	09:35		
10			OFF	OFF				

Figure 4-37: Selected Block Void User Rows

4. Click on the 

button. All users will be voided (see Figure 4-38).



	Last Name	Dept Group	On Off	Local APB	Enroll Date	Enroll Time	Void Date	Void Time
1	Polk	Management	OFF	ON	09/23/1998	09:21	09/23/1998	09:38
2	Adams	Support	ON	ON	09/23/1998	09:29		
3	Roosevelt	Manufacturing	ON	ON	09/23/1998	09:29		
4	Roosevelt	Accounting	OFF	ON	09/23/1998	09:29	09/23/1998	09:42
5	Lincoln	Management	OFF	OFF	09/23/1998	09:29	09/23/1998	09:42
6	Washington	Management	OFF	OFF	09/23/1998	09:29	09/23/1998	09:42
7	Franklin		OFF	ON	09/23/1998	09:35	09/23/1998	09:42
8	Hamilton		ON	ON	09/23/1998	09:35		
9	Jefferson		ON	ON	09/23/1998	09:35		
10			OFF	OFF				

Figure 4-38: Block Voided Users

5. Click on the 

button. If the voided users are not saved before clicking any other button or exiting the Setup Users spreadsheet window, the changes are lost and must be re-entered.

6. Now update the access control network with the new information. Click on the 

button on the tool bar (for details on the update process refer to “Update the Network” on page 35 in section 5).

2.2.7 Deleting Users – Dialog Box Method

The delete users feature allows an operator to remove users (including their card) from the user spreadsheet. Cards that have been deleted from the database must be re-enrolled before they can be reused in the access control system.

NOTE: Although deleted users and cards are removed from the user spreadsheet, they remain in the user database and all events involving those users/cards remain in the events data file. Event reports can be performed, locating past events that involved any deleted users/cards.

1. Scroll up and down the list of available users and locate the one to be deleted.
2. Click on the **Last Name** cell, or any cell on that user row.
3. Click on the 

button. A deletion confirmation window appears (see Figure 4-39).

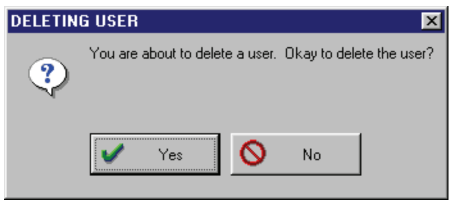
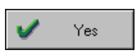


Figure 4-39: Deleting User Confirmation Window

4. Click on the 

button. The user entry in the database is removed and all other entries move up one row (see Figure 4-40).

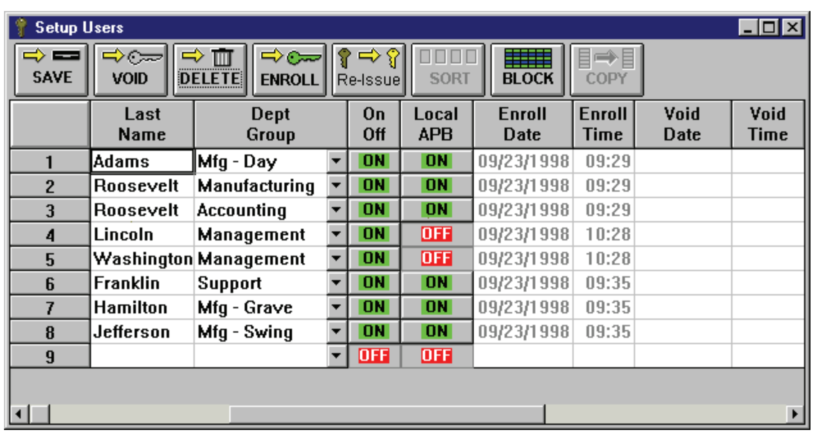
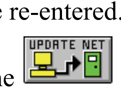


Figure 4-40: Deleted User

5. Click on the 

button. If the deleted card is not saved before clicking any other button or exiting the Setup Users spreadsheet window, the changes are lost and must be re-entered.

6. Now update the access control network with the new information. Click on the 

button on the tool bar (for details on the update process refer to “Update the Network” on page 35 in section 5).

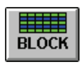
2.2.8 Block Deleting Users

The Block and Delete buttons allow an operator to select a number of voided users to be deleted all at one time, erasing all database references to those users and their cards. Cards that have been deleted from the database must be re-enrolled if they are to be reused in the access control system.

NOTE: Although deleted users and cards are removed from the user spreadsheet, they remain in the user database and all events involving those users/cards remain in the events data file. Event reports can be performed, locating past events that involved any deleted users/cards.

1. Click on one of the following cells from the first user row to be deleted.

- Last Name
- First
- Middle
- Enroll Date
- Enroll Time
- Void Date
- Void Time

2. Click on the 

button (see Figure 4-41).



Figure 4-41: Select the First Block Delete User

3. There are three ways to block select the users to be deleted. Use the method you find easiest.

- Click and hold on the first cell to copy and then drag the mouse down to the last user to delete.
- Click on the first cell, hold the Shift key down, and click on the last user to delete (see Figure 4-42 on page 36 of this section).
- Hold the Ctrl key down and one-at-a-time click on the users to be deleted. This method is best used when users are not in sequential order.

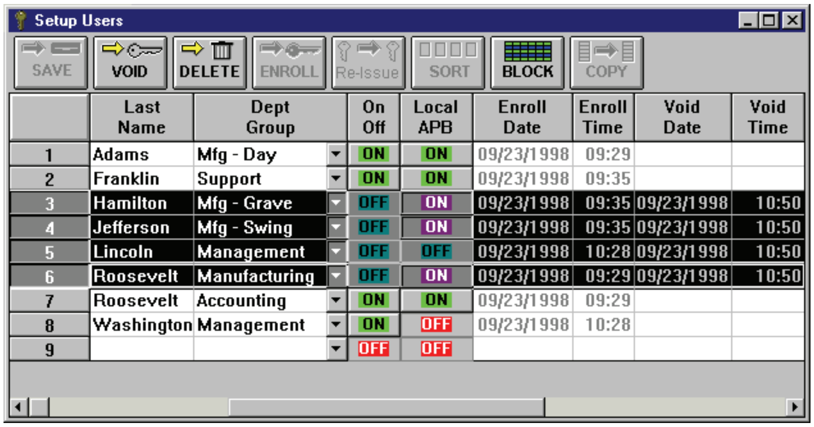


Figure 4-42: Selected Block Delete User Rows

4. Click on the DELETE button. A deletion confirmation window appears (see Figure 4-43).

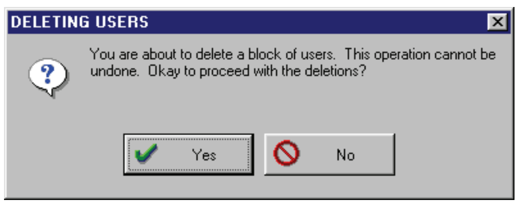


Figure 4-43: Block Deletion Confirmation Window

5. Click on the Yes button. The selected user/card entries in the database are now deleted and all other entries move up one row (see Figure 4-44).

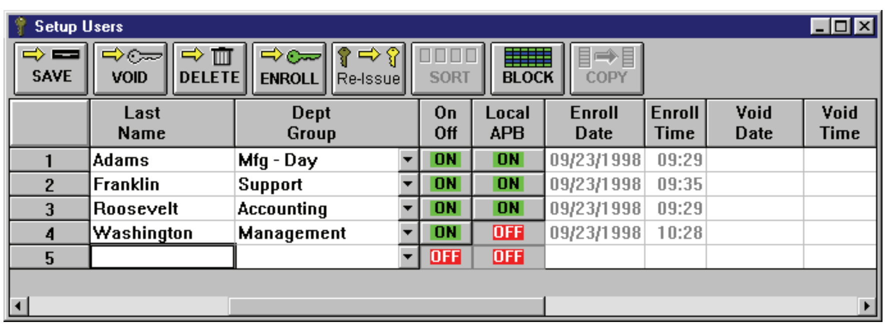


Figure 4-44: Block Deleted User

6. Click on the SAVE button. If the deleted cards are not saved before clicking any other button or exiting the Setup Users spreadsheet window, the changes are lost and must be re-entered.

7. Now update the access control network with the new information. Click on the UPDATE NET button on the tool bar (for details on the update process refer to "Update the Network" on page 35 in section 5).

2.2.9 Reissuing User Data

The Re-Issue User Data button transfers user data from one row in the spreadsheet (corresponding to one user) to another row in the spreadsheet. This allows an existing user in the spreadsheet to be reissued to a different card. No card enrollment or data entry is required. Click on the Re-Issue button to begin the process. Once a user is reissued all user databases are automatically saved.

Typically this is done when users lose or damage their cards and must be reissued to a new card quickly. Since no card enrollment is required, this process assumes there is an enrolled, unassigned card available to which reissuing can be done. If there is no such available card, enroll a card before proceeding with the re-issue (see “Card Enrollment” on page 3 of this section).

Reissuing user data is done in three steps.

- Select a row from which to copy data.
- Select a row to which to copy data.
- Perform the reissue/copy command.

In the following example Benjamin Franklin has lost a card and will be reissued to an enrolled but unassigned card in the spreadsheet.

1. Click on the 

button - a window similar to Figure 4-45 appears.
2. To exit the reissue process once the process has begun click on the 

button in the Reissue User Data window.

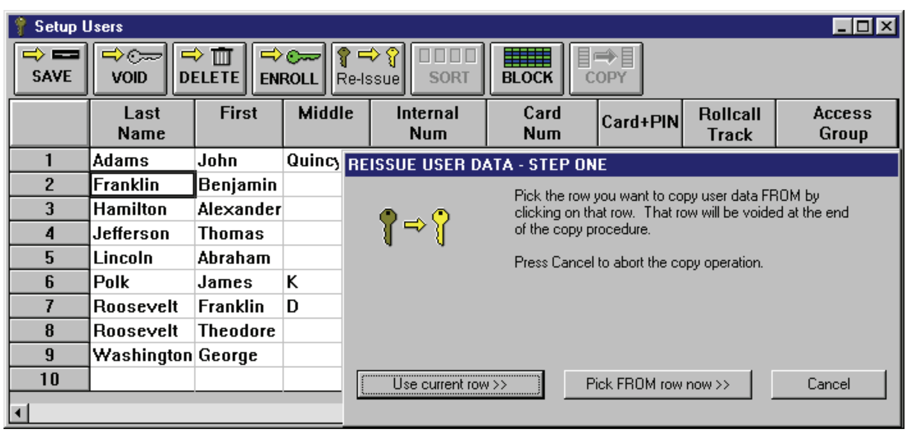


Figure 4-45: Reissue User Data – Step One

3. If any cell in the row for the user that will be reissued a card is highlighted (as shown in Figure 4-45) click on the 

button. If a different user is desired, click on the 

button and the Setup Users spreadsheet appears. Scroll through the list of users and click on a cell for the user that will be reissued a card (see Figure 4-45). A window similar to Figure 4-46 on page 38 of this section appears.

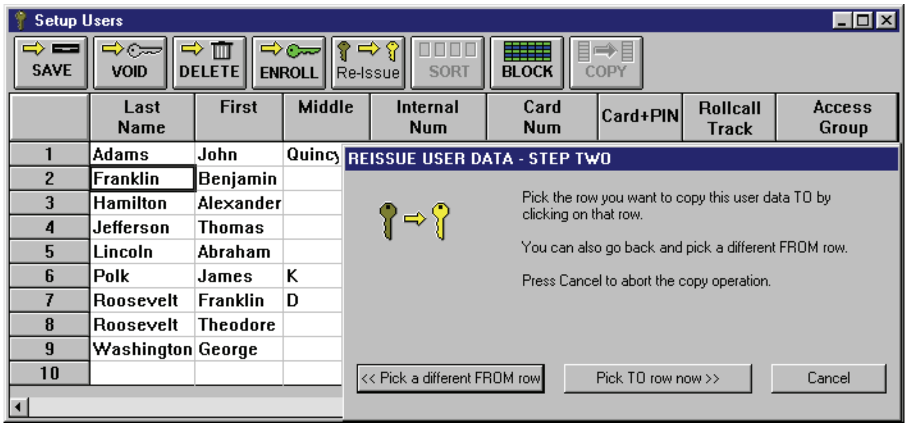


Figure 4-46: Reissue User Data – Step Two

4. If a different FROM row is desired, click on the [<< Pick a different FROM row] button and repeat Step 3. Otherwise, click on the [Pick TO row now >>] button and the Setup Users spreadsheet appears.
5. Scroll through the list of users and click on a cell for the row to which the user will be reissued.
6. If you selected a TO row that is already in use by another active user, the reissue error window appears (see Figure 4-47).

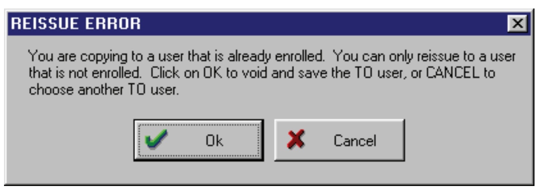


Figure 4-47: Reissue Error

7. To void the user you have selected as the TO row and reissue the other user over it, click on the [Ok] button. To cancel the TO row and return to the previous screen to select another TO row, click on the [Cancel] button. Click on the [Pick TO row now >>] button and repeat step 5.
8. If you have selected an available TO row, the copy user data window appears (see Figure 4-48)

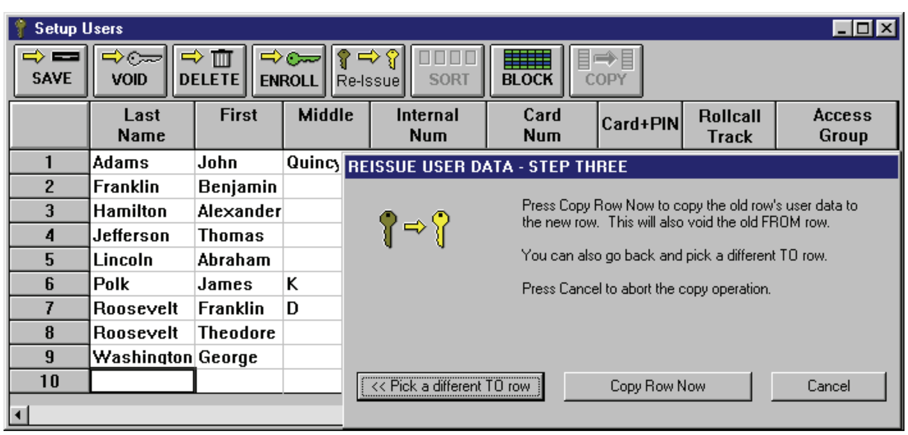
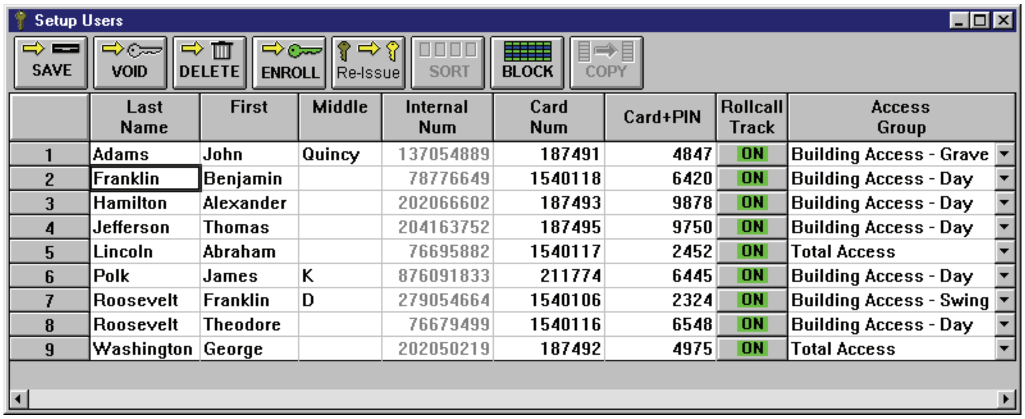


Figure 4-48: Reissue User Data – Step Three

9. If a different TO row is desired, click on the << Pick a different TO row button and repeat Step 5. Otherwise, click on the Copy Row Now button. The user data is copied to the TO row, the user and card in the FROM row is voided and deleted, and the user database is updated (as if the SAVE button was clicked – see Figure 4-49).



	Last Name	First	Middle	Internal Num	Card Num	Card+PIN	Rollcall Track	Access Group
1	Adams	John	Quincy	137054889	187491	4847	ON	Building Access - Grave
2	Franklin	Benjamin		78776649	1540118	6420	ON	Building Access - Day
3	Hamilton	Alexander		202066602	187493	9878	ON	Building Access - Day
4	Jefferson	Thomas		204163752	187495	9750	ON	Building Access - Day
5	Lincoln	Abraham		76695882	1540117	2452	ON	Total Access
6	Polk	James	K	876091833	211774	6445	ON	Building Access - Day
7	Roosevelt	Franklin	D	279054664	1540106	2324	ON	Building Access - Swing
8	Roosevelt	Theodore		76679499	1540116	6548	ON	Building Access - Day
9	Washington	George		202050219	187492	4975	ON	Total Access

Figure 4-49: Reissued User

2.2.10 Resizing Columns and Rows

If a cell is too small to display all the data in the cell, the spreadsheet's columns and rows can be resized by dragging a column or row boundary to a size that displays all the information.

While within the cells of the spreadsheet, the mouse cursor looks like a small cross.
When the mouse cursor hits a resizeable column or row boundary it will change to for a column and for a row.

NOTE: Resizing is temporary. When you close the window, all columns and rows will return to the default layout.

2.2.10.1 To Resize a Column

1. Locate the right boundary for a column. The mouse cursor will change to .
2. Click, hold and drag the mouse to the left of the window to make the column smaller, and to the right to make the column larger.
3. Release the mouse button and the new column size is set.

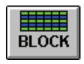
2.2.10.2 To Resize a Row

1. Locate the bottom boundary for a row. The mouse cursor will change to .
2. Click, hold and drag the mouse to toward the top of the window to make the row smaller, and to the bottom to make the row larger.
3. Release the mouse button and the new row size is set.

2.2.11 Printing User Data from the Spreadsheet (Quick Print)

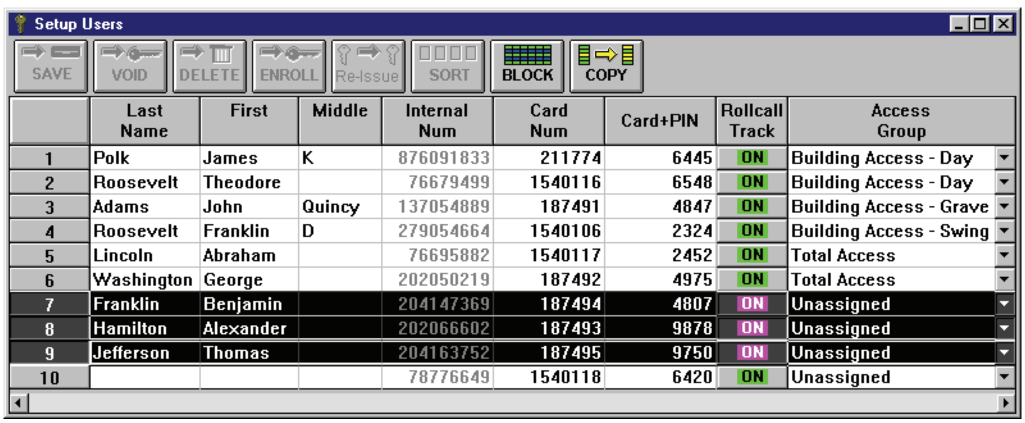
Selected sequential rows from the spreadsheet can be printed if desired. Because of the number and width of columns required for each user, printing user data typically requires two to three sheets of paper to display all the information for each user.

NOTE: Before printing user data from the spreadsheet, ensure the spreadsheet printer font has been set. This ensures the user data will be printed in a legible, easy to read format (see "Set the Spreadsheet Font" on page 44 in section 2).

1. Locate the first row to be printed.
2. Click on a cell in that row that is block copyable (Card Num, Access Group, Dept Group, ON/OFF, Local APB). The Block button becomes active when a block copyable cell is clicked.
3. Click on the 

button.
4. There are three ways to block select the rows to be printed. Use the method you find easiest.

- Click and hold on the first row and then drag the mouse down to the last row.
- Click on the first row, hold the Shift key down, and click on the last row (see Figure 4-50).
- Hold the Ctrl key down and one-at-a-time click on the users to be printed. This method is best used when users are not in sequential order.



	Last Name	First	Middle	Internal Num	Card Num	Card+PIN	Rollcall Track	Access Group
1	Polk	James	K	876091833	211774	6445	ON	Building Access - Day
2	Roosevelt	Theodore		76679499	1540116	6548	ON	Building Access - Day
3	Adams	John	Quincy	137054889	187491	4847	ON	Building Access - Grave
4	Roosevelt	Franklin	D	279054664	1540106	2324	ON	Building Access - Swing
5	Lincoln	Abraham		76695882	1540117	2452	ON	Total Access
6	Washington	George		202050219	187492	4975	ON	Total Access
7	Franklin	Benjamin		204147369	187494	4807	ON	Unassigned
8	Hamilton	Alexander		202066602	187493	9878	ON	Unassigned
9	Jefferson	Thomas		204163752	187495	9750	ON	Unassigned
10				78776649	1540118	6420	ON	Unassigned

Figure 4-50: Data Rows Selected to Print

5. On the menu bar, click on File ⇒ Print.
6. The highlighted data rows are now printed.

NOTE: If the Card+PIN feature has been enabled, it will print using this method. If a PIN number associated with a card becomes known to anyone other than the user, the security of the card is greatly decreased. Before printing in this method, you may want to disable the Card+PIN view feature (see "Set Card+PIN (P-650) Mode" on page 22 in section 2).

3.0 Identify an Unknown ID

The *Doors* program is able to read and identify a card's user in three different ways.

- reading the card at the enrollment reader
- entering the card's internal number
- entering the card's number – the number printed on the body of the card

NOTE: On a mixed PXL/EntraGuard system, the read card option is not available since there is no enrollment reader. You must use one of the other two methods to identify the user. However, when there is an EntraGuard unit on the system, a fourth option is added to identify a user by User ID (see "Identify an Unknown User ID" on page 39 in section 10).

1. To identify an unknown user, click on the Reports ⇒ Find ID Card pull-down menu. The Find ID window appears (see Figure 4-51).

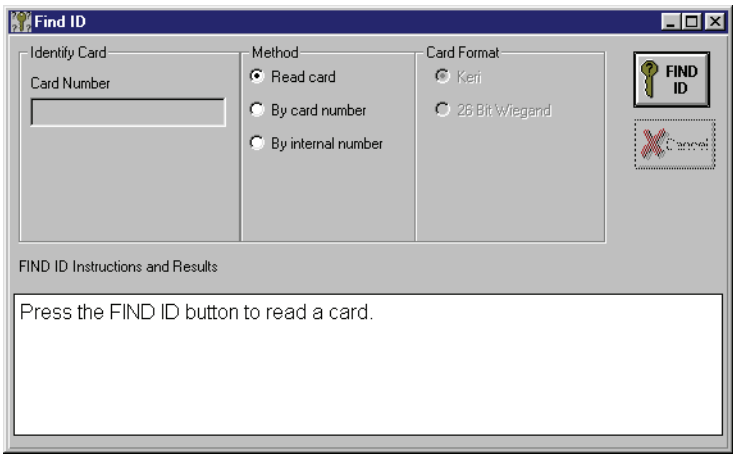


Figure 4-51: Find ID Window

3.1 Find ID by Reading the Card

This option may be used when you have a card and do not know to whom it is assigned.

NOTE: Find ID by reading a card cannot be performed using a P-650 Card+PIN Proximity Reader and Keypad.

1. Click on the **Read card** radio button.
2. Click on the  button.
3. Present the card to the enrollment reader.
4. The card's internal number, card number, facility code, to whom the card was previously assigned (if anyone), to whom the card is currently assigned and the date of issue is displayed in the "Find ID Instructions and Results" field (see Figure 4-52).

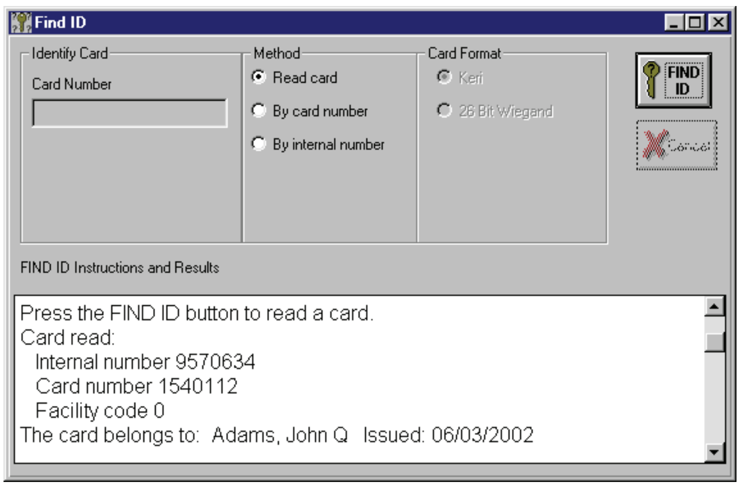


Figure 4-52: Card Identified by Reading

3.2 Find ID by Entering the Card Number

In this example, the operator has a card number and wants to identify whose card it is.

NOTE: This method is valid for K-series Keri Systems Proximity Cards (identified by a leading "K" on the body of the card) and W-series Keri Systems Wiegand Cards (identified by a leading "W" on the body of the card), see Figure 4-53.

1. Click on the **By card number** radio button.
2. Locate the Card Format field and click on the radio button corresponding to the card type: Keri (for Keri Proximity "K" Cards) or 26-bit Wiegand (for Keri Wiegand "W" Cards).
3. In the "Identify Card" field, locate and click in the "Card Number" cell.
4. Locate the card number on the body of the card. The card number is the second set of digits printed on the body of the card (in Figure 4-53, it is the digits corresponding to 1540115). The card number will be more than 4 digits long. In this example, the entire number of the card is K1559 1540115; the card number is 1540115, 6 digits long.

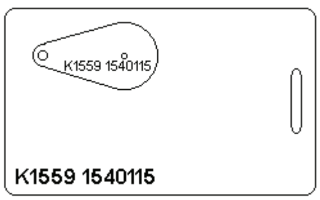


Figure 4-53: Proximity Card Number

5. Type the card's number in the "Card Number" cell.
6. Click on the  button.
7. The user's name and date of issue is displayed in the "Find ID Instructions and Results" field (see Figure 4-54).

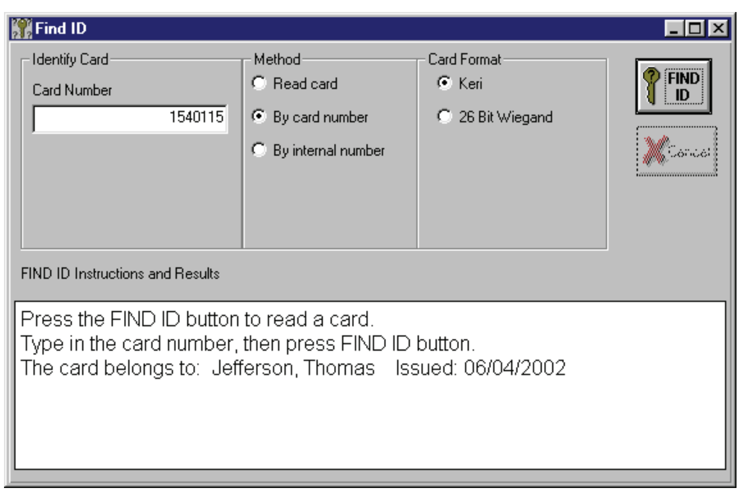


Figure 4-54: Card Identified by the Card Number

3.3 Find ID by Entering the Internal Number

In this example, the operator has a card's internal number and wants to identify whose card it is.

1. Click on the **By internal number** radio button.
2. Locate the Card Format field and click on the radio button corresponding to the card type: Keri (for Keri Proximity "K" Cards) or 26-bit Wiegand (for Keri Wiegand "W" Cards).
3. In the "Identify Card" field, locate and click in the "Card Number" cell.
4. Type the card's internal number in the "Card Number" cell.
5. Click on the  button.
6. The user's name and date of issue is displayed in the "Find ID Instructions and Results" field (see Figure 4-55).

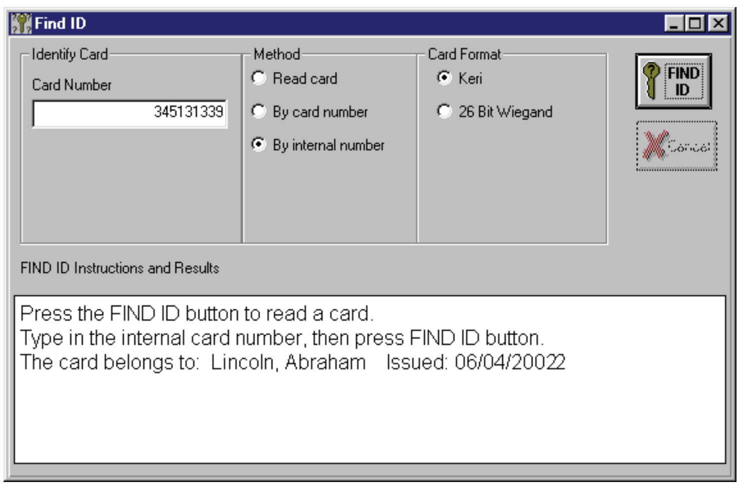


Figure 4-55: Card Identified by the Internal Number

This page has been intentionally left blank.

Section 5

Monitor and Update

1.0 Setup Monitor Windows and Events

The setup monitor and events commands allow an operator to perform six tasks.

- enable/disable host computer auto-collection of events from controllers
- configuration of up to three event monitor windows
- selecting which events should be stored in the event file in the host computer's hard disk
- selecting which events should be stored and reported by controllers in the access control network
- selecting one of three event file types for archiving event files
- archiving old events freeing up space on the host computer's hard disk

1. To access the setup monitor and events commands, click on the Setup ⇒ Monitor and Events pull-down menu.
2. Click on the **Monitoring Options** tab. The Setup Monitor window appears (see Figure 5-1).

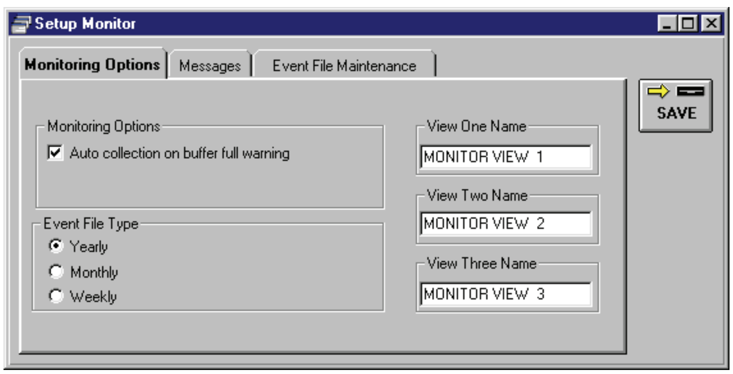


Figure 5-1: Setup Monitor and Events Window

1.1 Enable/Disable Auto-Collection

The Auto-collection on buffer full option allows an operator to define if the host computer is expected to receive event information from the controller's event memory buffer when the controller's buffer becomes full. This ensures that as new events are received, the oldest events are not deleted to make room for the new events. If the controller's buffer reaches the buffer limit, the controller uploads its buffer contents to the host computer, clearing the buffer.

NOTE: These instructions configure the Doors software for receiving information from the controller, but the controller must also be configured to transmit this information. This is done in "Set Controller Dial-Out Parameters" on page 21 in section 3. Both steps must be done for proper uploading of information from a controller to the host computer/Doors software.

1. To enable auto-collection, click on the check box beside the "Auto-collection on buffer full warning" option in the "Monitoring Options" field. When the box has a check mark, auto-collection is enabled (see Figure 5-2 on page 5 of this section).
2. To disable auto-collection, click on the check box beside the "Auto-collection on buffer full warning" option in the "Monitoring Options" field. When the box does not have a check mark, auto-collection is disabled (see Figure 5-1 on page 3 of this section). This is the default value.
3. Click on the 

button. If the auto-collection information is not saved before clicking any other button or exiting the setup monitor window, the data entered is lost and must be re-entered.

NOTE: When a controller attempts to connect with the host computer to upload the contents of its buffer and it is unable to connect, it will continue to try every 10 minutes until it connects. This is done to prevent the event buffer from overflowing and losing the oldest events in the buffer. If the buffer fills and new events are recorded, the oldest events in the buffer are overwritten by the newest events. In order for the host computer to receive information from the controller, the host computer must be on and the Doors program must be opened.

1.2 Configure Event Monitoring Windows

Event monitoring allows an operator to configure up to three windows which display filtered, real-time events occurring on the access control system. This allows an operator to create custom monitoring windows, each dedicated to monitoring specific types of events.

There are four processes involved in configuring event windows: naming the event monitoring windows, editing the event message text strings, assigning the events to be tracked by the monitoring windows, and assigning sound alerts to events.

1.2.1 Naming Event Monitoring Windows

The View One Name, View Two Name, and View Three Name fields allow an operator to assign a descriptive name of up to 32 characters for each of the three monitor screens. In this example, the view three name field will be named for monitoring door access events.

1. Click in the **View Three Name** field.
2. Delete the **MONITOR VIEW 3** name in the field (use any combination of backspaces, deletes, and highlighting and deleting to clear the text out of the field).
3. Type **Door Access Events**. The resulting window should look similar to Figure 5-2.

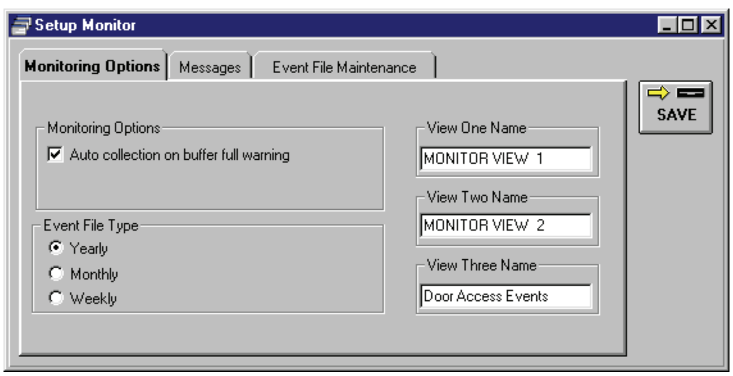


Figure 5-2: Naming Monitor View Three

4. Click on the  button. If the naming event monitoring information is not saved before clicking any other button or exiting the setup monitor window, the data entered is lost and must be re-entered.

1.2.2 Message Text Strings

There are 160 possible events that can be tracked. Each event is identified by a message text string that is a brief description of the event generated by the controller when the event occurs. These strings can be edited; an operator can change the message that is displayed when an event occurs. There is a 40 character maximum for these text strings. This allows an operator to create a message string that is more descriptive to the operator, making report viewing easier.

NOTE: For information on Alarm Control Event Messages, see "Alarm Control" on page 1 in section 12.

1.2.2.1 Editing Message Text Strings

1. To access the message text strings, click on the Setup ⇒ Monitor and Events pull-down menu.
2. Click on the **Messages** tab. The Messages window appears (see Figure 5-3).

NOTE: The "Elevator Reports Event" column does not appear unless elevator control has been activated in "Set Door Type" on page 17 in section 2.

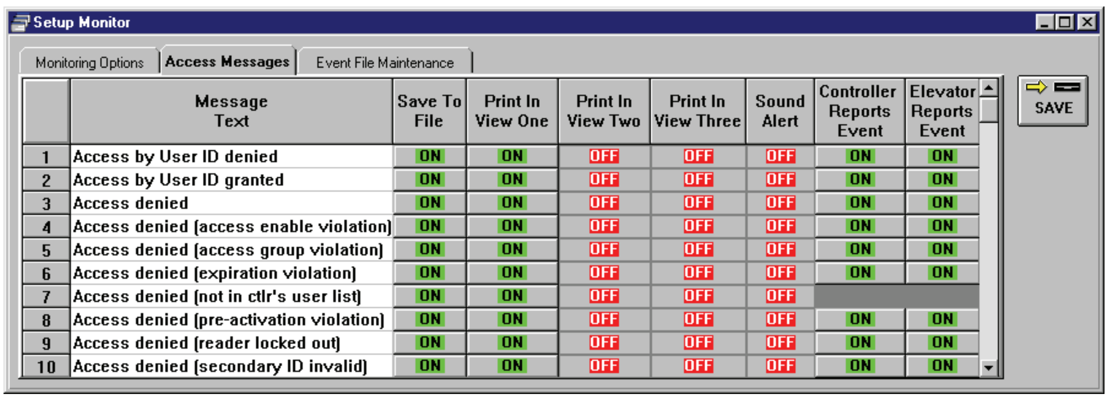


Figure 5-3: Event Messages and Configuration Fields

3. Use the scroll bar at the right side of the window to scroll through the entire list of event messages and locate the message text string you would like to rename.
4. Click in the cell and type the new message text string name.

NOTE: When changing message text fields, the operator must be cautious that the intent of the original message (the event that occurred to generate the message) is not changed when a new message is defined. Otherwise other operators may misinterpret the redefined event message. <u>There is no default reset of the messages to return the text to its original form.</u>

5. Click on the  button. If the message text change is not saved before clicking any other button or exiting the Setup Monitor window, the data entered is lost and must be re-entered.

1.2.2.2 Message Text String Definitions

Access By User ID Denied
Reported whenever an invalid User ID is entered into the EntraGuard controller in an attempt to gain access to a controlled door.

Access By User ID Granted
Reported whenever a valid User ID is entered into the EntraGuard controller, which then grants the user access to a controlled door.

Access Denied
Reported whenever an invalid card is presented to a door/controller in an attempt to gain access to a controlled area.

Access Denied (Alarm System Armed)
Reported whenever an invalid card is presented to a door/controller in an attempt to gain access to a controlled area when the alarm system is armed.

Access Denied (Access Enable Violation)
Reported whenever a card is presented to a reader that is not enabled in the Setup System Doors tab.

Access Denied (Access Group Violation)
Reported whenever a card is presented to a reader that is assigned an access group that is not given permission to access that door.

Access Denied (Expiration Violation)
Reported whenever a card is presented to a reader after the expiration date has passed.

Access Denied (Not in Ctlr's User List)
Reported whenever a user in the Doors database tries to gain access to a door not in their access group.

Access Denied (Pre-Activation Violation)
Reported whenever a temp user attempts to gain access before the activation date has been reached.

Access Denied (Reader Locked Out)
Reported whenever a Primary ID and Secondary ID combination has been entered incorrectly 6 times in a row and the reader/keypad is locked out for the period of time pre-set on the System Options Tab in *Doors*.

Access Denied (Secondary ID Invalid)
Reported whenever a Secondary ID is entered that does not match the Primary ID.

Access Denied (Secondary ID Null)
Reported whenever a user has been assigned the Secondary Status of "No Access".

Access Denied (Secondary ID Timeout)
Reported whenever a user has failed to enter a Secondary ID within the time limit set on the Doors Tab in *Doors*.

Access Granted
Reported whenever a valid card is presented to a door/controller, which then grants the user access to a controlled area.

Access Group Changed
Reported whenever an operator changes access group data.

Access Group Deleted
Reported whenever an operator deletes an access group.

All Doors Locked
Reported whenever the access control network performs a Global Secure command, locking all non-timezone controlled doors in the access control network.

All Doors Unlocked
Reported whenever the operator performs a Global Unlock command, unlocking all doors in the access control network.

Amnesty Granted
Reported whenever a user is granted APB amnesty at a controller and is allowed access.

APB Violation
Reported whenever a card was used twice-in-a-row at a door in an attempt to gain access to a secured area without first leaving that area. This prevents a user from using a valid card to enter a controlled area and then passing that card back for another person to use to enter that area.

Auto Collect Flag Off
Reported if the "Auto collection on buffer full warning" feature has not been enabled, configuring the host computer to receive event data from controllers.

Auto Lock Restored
Reported whenever an operator restores a controller/door's automatic locking feature.

Auto Lock Suspended
Reported whenever an operator suspends a controller/door's automatic locking feature.

Autoconfig Performed
Reported whenever an operator performs the autoconfiguration command, polling all controllers for information used to create the controllers database.

Card+PIN (P-650) PIN Entry Violation
Reported whenever a user's attempt to enter a PIN after presentation of an access card is incorrect. To be used only in connection with a P-650 Card+PIN Proximity Reader and Keypad.

Connect Refused - PIN
Reported whenever an operator's attempt to log into a remote site was refused by the site's master controller because the operator did not enter the correct personal identification number (PIN) for the site.

Connect Refused - Site
Reported whenever an operator's attempt to log into a remote site was refused by the site's master controller because the operator does not have the authorization to access the site.

Ctlr Cold Reset
Reported if a cold reset (power cycling off and then on) occurs at a controller.

Ctlr Com Restored
Reported whenever communication with a remote site's master controller is made.

Ctlr Comm Failure
Reported if communication with a remote site's master controller was lost unexpectedly.

Ctlr Did Not Respond
Reported if a command is sent to a remote site's master controller, but the controller does not respond, acknowledging it received the command.

Ctlr Event Threshold
Reported by a controller whenever that controller reaches its event buffer threshold and it needs to transfer/clear data from its buffer.

Ctlr Hard Reset
Reported if a hard reset (someone physically resetting the controller) occurs at a controller.

Ctlr Internal Error
Reported if a controller has an unidentifiable internal error.

Ctlr IO File Changed
Reported whenever an operator changes controller Input/Output data definitions.

Ctlr Key DB Corrupt
Reported if a controller's keypad database (used for secondary verification of a cardholder) is corrupt, invalidating its data.

Ctlr Mem Corrupted
Reported if a controller's RAM memory is corrupted, disrupting controller operation.

Ctlr Self Test Failed
Reported if a controller's power on self-test (POST) fails, or if a controller's supply power either falls too low or raises too high for proper operation.

Ctlr Warm Reset
Reported if a controller's "watch-dog" timer expires (indicating the controller might be hung).

Ctlr/Door File Changed
Reported whenever an operator changes controller/door configuration information.

Daylight Savings Off
Reported when the controller's clock disables the one-hour time change for daylight savings time.

Daylight Savings On
Reported when the controller's clock enables the one-hour time change for daylight savings time.

Door Closed
Reported whenever a door closes following a valid access request.

Door Forced Open
Reported if a door has been forced open without a valid access request having been made.

Door Locked
Reported whenever a controller locks a door.

Door Locked by Operator
Reported whenever a door physically locks following a manual lock command issued by an operator.

Door Locked: Local Tele Cmd
Reported whenever an EntraGuard controlled door is locked using a telephone command code.

Door Locked: Remote Tele Cmd
(This message is reserved for future use.)

Door Momentary Unlocked: Remote Tele Cmd
(This message is reserved for future use.)

Door Not Opened
Reported if a door is not opened within the Unlock Time following a valid access request.

Door Opened
Reported whenever a door is opened following a valid access request.

Door Opened Too Long
Reported if a door is held open beyond the Open Time following a valid access request.

Door Report Created
Reported whenever an operator requests a door report to be generated for review or printing.

Door Unlocked
Reported whenever a controller unlocks a door.

Door Unlocked by Operator
Reported whenever a door physically unlocks following a manual unlock command issued by an operator.

Door Unlocked: Key Override Switch
(This message is reserved for future use.)

Door Unlocked: Local Tele Cmd
Reported whenever an EntraGuard controlled door is unlocked using a telephone command code.

Door Unlocked: Remote Tele Cmd
(This message is reserved for future use.)

Doors Disconnected
Reported if a door/controller is disconnected from the access control network.

Dual Access Denied
(This message is reserved for future use.)

Dual Access Granted
(This message is reserved for future use.)

Duress Alert
Reported whenever the * key is selected on a Pyramid reader (set in 8-Bit Burst mode).

EG Unit: Local Phone Connect Attempted
Reported whenever the EG Unit attempts a connection with a tenant's phone.

Event Report Created
Reported whenever an operator requests a event report to be generated for review or printing.

Global Amnesty Granted
Reported whenever global amnesty is granted to all the controllers on a network.

Global Lock OFF
Reported whenever an operator disables the global lock command.

Global Lock ON
Reported whenever an operator enables the global lock command.

Global Secure Lock
Reported whenever a controller is locked by a global secure lock command performed by the system per the time set in Global Secure.

Global Unlock Off
Reported whenever an operator disables the global unlock command.

Global Unlock On
Reported whenever an operator enables the global unlock command.

Holiday List Changed
Reported whenever an operator changes holiday list names or dates.

Host Comm Failed
Reported if a controller loses communication with the host computer.

Input Point Off
Reported whenever an input point on a controller changes state from active to inactive.

Input Point On
Reported whenever an input point on a controller changes state from inactive to active.

Interphone
(This message is reserved for future use.)

Link Active
Reported whenever a communication link is established between the host computer and the master controller at a remote site.

Link File Changed
Reported whenever an operator changes controller Input/Output link data definitions.

Monitor File Changed
Reported whenever an operator changes any of the three system monitor window definition.

Monitor Started
Reported whenever an operator starts any of the three system monitor windows.

Monitor Stopped
Reported whenever an operator stops any of the three system monitor windows.

Net Connect Accepted
Reported whenever an operator's request to connect to a remote site is accepted by the remote site's master controller.

Net Connect Made
Reported whenever the host computer connects to a remote site.

Net Connect Request
Reported whenever an operator makes a request to connect to a remote site.

Net Disconnected
Reported whenever a remote site disconnects from the host computer.

Net Requested Collect
Reported whenever a remote site requests to upload a controller's event buffer contents to the host computer.

Operator Added Site
Reported whenever an operator adds a new remote site to the access control database.

Operator Created Report
Reported whenever an operator performs one of the reporting options.

Operator Deleted Site
Reported whenever an operator deletes a remote site from the access control database.

Operator Did Smart Update
Reported whenever an operator performs a smart update (uploading only database values that have changed since the last update).

Operator Did Update
Reported whenever an operator performs a complete update (uploading all database information).

Operator Exports Users To Text File
Reported whenever an operator uses the User Data File Export/Import feature to export user data to a text file.

Operator File Changed
Reported whenever an operator rights file has been created or edited.

Operator Granted Global Amnesty
Reported whenever an operator manually grants amnesty to all users in the access control network.

Operator Granted User ID Amnesty
Reported whenever an operator manually grants amnesty to a single user.

Operator Imports Users From Text File
Reported whenever an operator uses the User Data File Export/Import button to import user data from a text file.

Operator Locked Door
Reported whenever an operator performs an immediate lock door command.

Operator Logged Off
Reported whenever an operator logs off the *Doors* program.

Operator Logged On
Reported whenever an operator logs on the *Doors* program.

Operator Modified Site
Reported whenever an operator modifies/changes any of the operating parameters for a site.

Operator Pulsed Door
Reported whenever an operator pulses a door lock (temporarily unlocking the door to allow momentary, immediate entrance).

Operator Requested Collect
Reported whenever an operator requests event data from controllers.

Operator Restored Auto Unlock/Lock Timezone
Reported whenever an operator restores/enables an auto unlock/lock timezone.

Operator Restored Output
Reported whenever an operator restores/enables an output point.

Operator Set Network Time
Reported whenever an operator performs the set time command, synchronizing the time and date tracked by all the controllers to the time and date tracked by the host computer.

Operator Shut Off Alert Sound
Reported whenever an operator acknowledges an alert by clicking on the sound alert icon on the tool bar.

Operator Suspended Auto Unlock/Lock Timezone
Reported whenever an operator suspends an auto unlock/lock timezone.

Operator Turn Off Alarm Control Option
Reported whenever an operator turns off the alarm control option.

Operator Turn Off Dual Verification Option
Reported whenever an operator turns off the dual verification option.

Operator Turn Off Elevator Option
Reported whenever an operator turns off the elevator door option.

Operator Turn Off Gate Option
Reported whenever an operator turns off the gate option.

Operator Turn Off Temp Users Option
Reported whenever an operator turns off the temp users option.

Operator Turn Off Time and Attendance Terminal Option
Reported whenever an operator turns off the time and attendance terminal option.

Operator Turn On Alarm Control Option
Reported whenever an operator turns on the alarm control option.

Operator Turn On Dual Verification Option
Reported whenever an operator turns on the dual verification option.

Operator Turn On Elevator Option
Reported whenever an operator turns on the elevator door option.

Operator Turn On Gate Option
Reported whenever an operator turns on the gate option.

Operator Turn On Temp Users Option
Reported whenever an operator turns on the temp users option.

Operator Turn On Time and Attendance Terminal Option
Reported whenever an operator turns on the time and attendance terminal option.

Operator Turned Off Daylight Savings Adjust Option
Reported whenever an operator disables the daylight savings adjust option.

Operator Turned Off Global Lock Option
Reported whenever an operator disables the global lock command.

Operator Turned Off Global Unlock Option
Reported whenever an operator disables the global unlock command.

Operator Turned Off LAPB
Reported whenever an operator turns off the local anti passback feature.

Operator Turned Off Sites
Reported whenever an operator turns off the multiple sites feature.

Operator Turned On Daylight Savings Adjust Option
Reported whenever an operator enables the daylight savings adjust option.

Operator Turned On Global Lock Option
Reported whenever an operator enables the global lock command.

Operator Turned On Global Unlock Option
Reported whenever an operator enables the global unlock command.

Operator Turned On LAPB
Reported whenever an operator turns on the local anti passback feature.

Operator Turned On Sites
Reported whenever an operator turns on the multiple sites feature.

Operator Turned Output Off
Reported whenever an operator manually turns off an output point.

Operator Turned Output On
Reported whenever an operator manually turns on an output point.

Operator Unlocked Door
Reported whenever an operator performs an immediate unlock door command.

Output 1 Momentary ON: Local Tele Cmd
Reported whenever the Output 1 is activated using a telephone command code.

Output 1 Momentary ON: Remote Tele Cmd
(This message is reserved for future use.)

Output 1 OFF: Remote Tele Cmd
(This message is reserved for future use.)

Output 1 ON: Remote Tele Cmd
(This message is reserved for future use.)

Output 2 Momentary ON: Local Tele Cmd
Reported whenever the Output 2 is activated using a telephone command code.

Output 2 Momentary ON: Remote Tele Cmd
(This message is reserved for future use.)

Output 2 OFF: Remote Tele Cmd
(This message is reserved for future use.)

Output 2 ON: Remote Tele Cmd
(This message is reserved for future use.)

Output Point Off
Reported whenever an operator manually turns off an output point.

Output Point On
Reported whenever an operator manually turns on an output point.

Panel Armed
(This message is reserved for future use.)

Panel Disarmed
(This message is reserved for future use.)

Panel Tamper
(This message is reserved for future use.)

Pending on Exempt Secondary ID
Reported whenever a user assigned the Secondary Status of "Exempt" is granted access.

Request to Exit
Reported whenever a controller receives a request to exit signal.

Request to Exit #2
Reported whenever a controller receives an auxiliary request to exit signal.

Request to Exit #2 Continuous Off
Reported whenever a controller receiveds an auxiliary continuous request to exit signal.

TDD Output Turned Off
(This message is reserved for future use.)

TDD Output Turned On
(This message is reserved for future use.)

Timed Amnesty Granted
Reported whenever a controller grants amnesty based on a time interval.

Timezone Changed
Reported whenever an operator changes a timezone definition.

Timezone Deleted
Reported whenever an operator deletes a timezone.

Unknown Event
Reported if an event has occurred on the access control system that is not recognized by the controller firmware or by the access control software.

Unknown Key
Reported if an attempt was made to access a secure area with a card that is not recognized by the site’s access control network.

Unknown Message From Net
Reported if a message is received from the access control system that is not recognized by the access control software.

User Data File Changed
Reported whenever an operator changed user data.

User Data Report Created
Reported whenever an operator requests a user report to be generated for review or printing.

User ID Entry Violation: Too Many Tries
Reported whenever an invalid User ID has been entered too many times into the EntraGuard unit.

User ID Unknown
Reported whenever an unknown User ID is entered into the EntraGuard unit.

1.2.3 Assigning Events to be Monitored

The Print in View One, Two, and Three fields allows an operator to select the events that should be displayed in each of the three monitor windows. The default is for View One to display all events and for View Two and View Three to display no events.

Before assigning the events to be tracked by a monitor window, review the list of possible events and identify the events that should be tracked. In this example, view three will be configured for monitoring door access events. After reviewing the list of events, the following events will be selected for tracking in monitor window three.

- Access Denied
- Access Granted
- Door Closed
- Door Forced Open
- Door Locked
- Door Not Opened
- Door Opened
- Door Opened Too Long
- Door Unlocked

1. To access the assigning events to be monitored commands, click on the Setup ⇒ Monitor and Events pull-down menu.
2. Click on the **Messages** tab. The Messages window appears (see Figure 5-4).

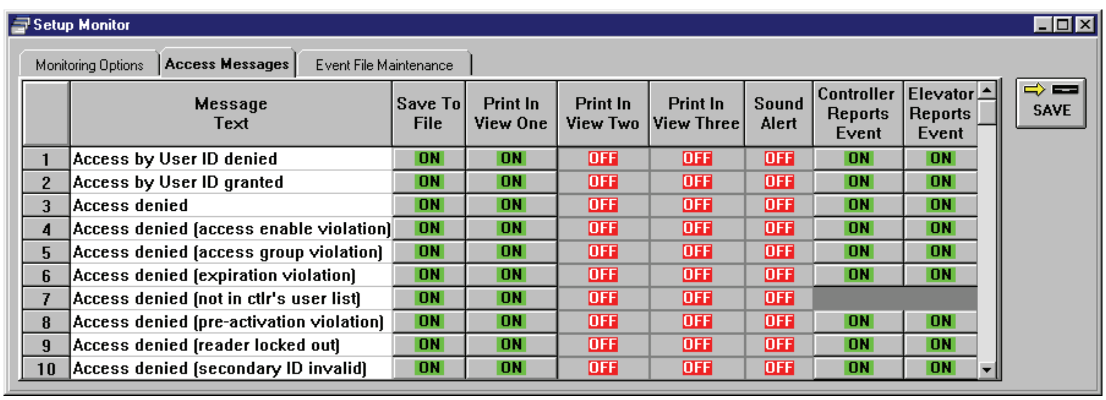


Figure 5-4: Event Messages and Configuration Fields

3. Reviewing the above list, scroll down the “Message Text” column and locate the “Access Denied” message text.
4. Scan across the access denied row to the “Print In View Three” column.
5. Click in the cell. It will change from an OFF button to an ON button.
6. Scroll down the “Message Text” column and locate the “Access Granted” message text.
7. Scan across the access granted row to the “Print In View Three” column.
8. Click in the cell. It will change from an OFF button to an ON button.
9. Repeat this process for the seven other message text strings.
10. The resulting window will look similar to Figure 5-5 on page 18 of this section.

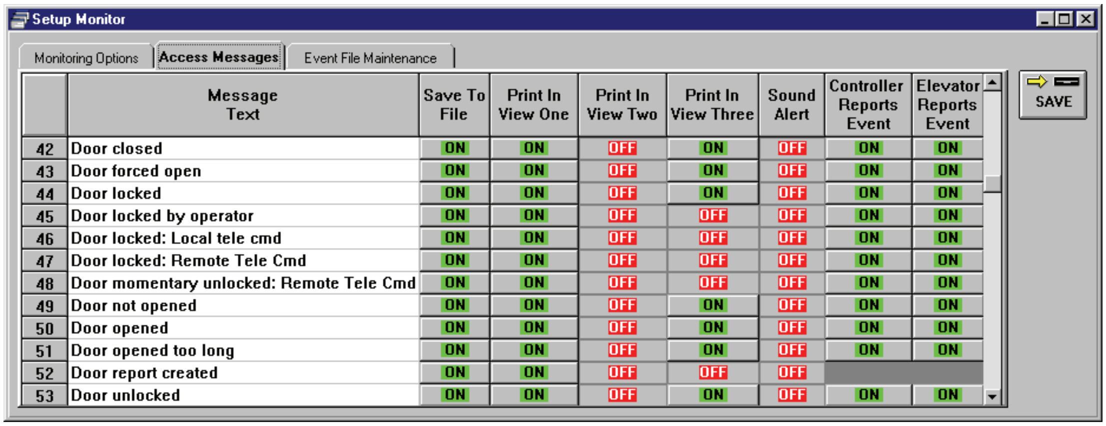


Figure 5-5: Monitor View Setup - Door Monitoring

11. To disable a print in view selection, locate the message text to be disabled. Scan across the text row to the print in view column to be disabled. Click in the cell. It will change from an ON button to an OFF button.
12. Click on the SAVE button. If the print in view change is not saved before clicking any other button or exiting the Setup Monitor window, the data entered is lost and must be re-entered.
13. From now on, when View Three event monitoring is started, only the selected events (listed at the beginning of this section) are displayed.

1.2.4 Sound Alert on Event

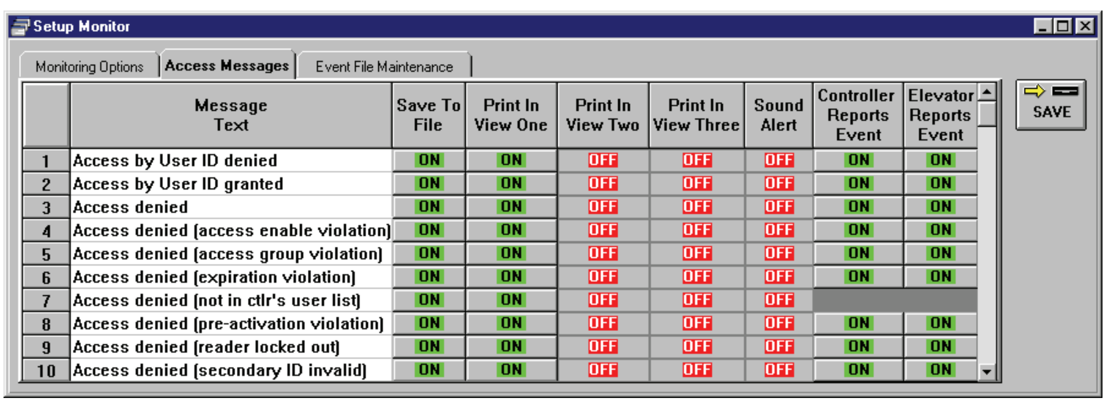
The sound alert on event fields allow an operator to designate events for sound annunciation when they occur. Any time a selected event occurs, the alarm sounds repeatedly until acknowledged by the operator. Sound alerts are only active when monitor mode is enabled; events collected from a controller's event buffer will not sound alerts. The default is for all sound alerts to be off. If the host computer has a sound card the Windows Exclamation sound plays (this is set in the Control Panel ⇒ Sounds window). If the host computer does not have a sound card the PC's speaker beeps.

Sound alert acknowledgement is done by clicking on the  button on the *Doors* tool bar (see "Acknowledging Sound Alerts" on page 46 of this section). When an event is selected for sound alert, all events of this type generate an alert; there is no filtering by input point, controller, door, or site.

NOTE: When using a sound card, once an alert sounds, the entire Windows Exclamation sound plays regardless of when the operator clicks on the  *button. Keri Systems recommends using a short duration Exclamation sound such as the default sound used by Windows.*

In this example, the Access Denied and Unknown Key event messages will be sound alert enabled. Enabling these two messages ensures that every invalid card presentation at a reader is annunciated.

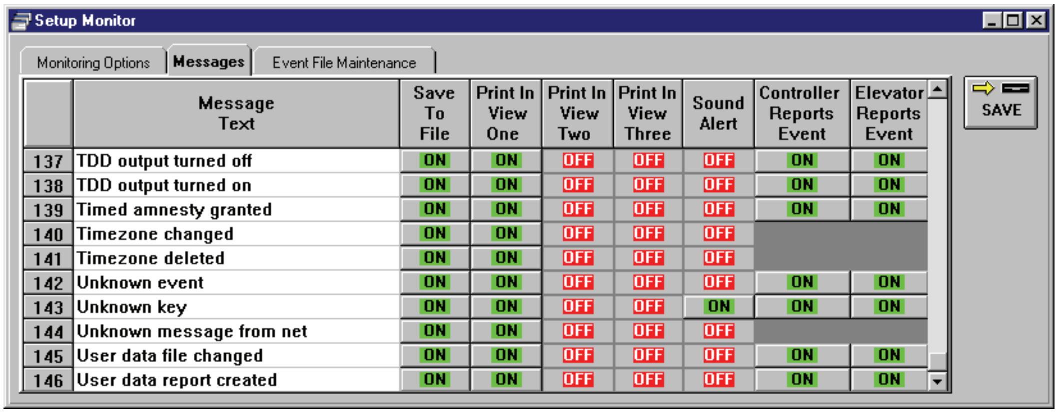
1. To access the events to be sound alert enabled, click on the Setup ⇒ Monitor and Events pull-down menu.
2. Click on the **Messages** tab. The Messages window appears (see Figure 5-6).



	Message Text	Save To File	Print In View One	Print In View Two	Print In View Three	Sound Alert	Controller Reports Event	Elevator Reports Event
1	Access by User ID denied	ON	ON	OFF	OFF	OFF	ON	ON
2	Access by User ID granted	ON	ON	OFF	OFF	OFF	ON	ON
3	Access denied	ON	ON	OFF	OFF	OFF	ON	ON
4	Access denied (access enable violation)	ON	ON	OFF	OFF	OFF	ON	ON
5	Access denied (access group violation)	ON	ON	OFF	OFF	OFF	ON	ON
6	Access denied (expiration violation)	ON	ON	OFF	OFF	OFF	ON	ON
7	Access denied (not in ctlr's user list)	ON	ON	OFF	OFF	OFF		
8	Access denied (pre-activation violation)	ON	ON	OFF	OFF	OFF	ON	ON
9	Access denied (reader locked out)	ON	ON	OFF	OFF	OFF	ON	ON
10	Access denied (secondary ID invalid)	ON	ON	OFF	OFF	OFF	ON	ON

Figure 5-6: Event Messages and Configuration Fields

3. Use the scroll bar on the right side of the window and scroll through the list of message texts until the "Access Denied" message text string appears.
4. Scan across that row to the Sound Alert column.
5. Click in the cell. It will change from an OFF button to an ON button.
6. Scroll through the Message Text column and locate the "Unknown Key" message text string.
7. Scan across that row to the Sound Alert column.
8. Click in the cell. It will change from an OFF button to an ON button (see Figure 5-7 on page 20 of this section).



Setup Monitor

Monitoring Options | Messages | Event File Maintenance

	Message Text	Save To File	Print In View One	Print In View Two	Print In View Three	Sound Alert	Controller Reports Event	Elevator Reports Event
137	TDD output turned off	ON	ON	OFF	OFF	OFF	ON	ON
138	TDD output turned on	ON	ON	OFF	OFF	OFF	ON	ON
139	Timed amnesty granted	ON	ON	OFF	OFF	OFF	ON	ON
140	Timezone changed	ON	ON	OFF	OFF	OFF		
141	Timezone deleted	ON	ON	OFF	OFF	OFF		
142	Unknown event	ON	ON	OFF	OFF	OFF	ON	ON
143	Unknown key	ON	ON	OFF	OFF	ON	ON	ON
144	Unknown message from net	ON	ON	OFF	OFF	OFF		
145	User data file changed	ON	ON	OFF	OFF	OFF	ON	ON
146	User data report created	ON	ON	OFF	OFF	OFF	ON	ON

Figure 5-7: Sound Alert Setup - Unknown Key

9. Click on the  button. If the sound alert change is not saved before clicking any other button or exiting the Setup Monitor window, the data entered is lost and must be re-entered.

Do NOT enable the "Operator Silenced Alert Sound" message. Enabling this message can cause an endless loop of alarm acknowledgement generating a new event to be acknowledged.

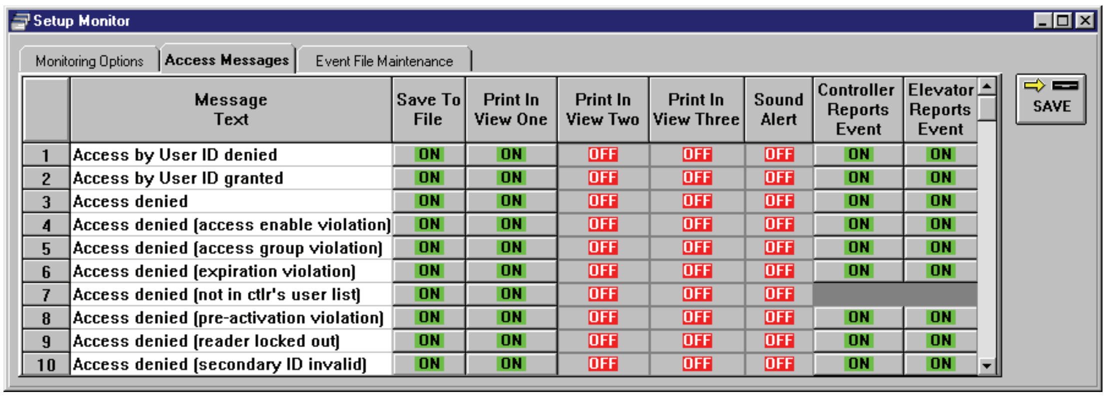
NOTE: When a card is presented to a controller that the controller does not recognize, the controller records an Unknown Key event message to the controller's event buffer. When the event buffer is downloaded to the host computer, the Doors program reviews the list of Unknown Key messages and compares the card ID numbers to the user list. Any Unknown Key messages associated with card IDs that are in the user list are converted to Access Denied messages. This differentiates between cards that are truly "unknown" to the system from cards being presented by a user in an attempt to access an area in which the user is not allowed.

1.2.5 Controller Reports Events

The controller reports events fields allow an operator to determine which events should be reported by the controller. Many events are normal day to day activities that an operator may not want to have take up controller processing time or event buffer space. The default is for all controller generated events to be stored and reported in the controller's event buffer.

In this example, the message text strings notifying when the controllers process the enabling/disabling of Daylight Savings time are disabled so they will not be stored and reported in the controller's event buffer.

1. To access the message text strings to not be stored and reported in the controller's event buffer, click on the Setup ⇒ Monitor and Events pull-down menu.
2. Click on the **Messages** tab. The Messages window appears (see Figure 5-8).



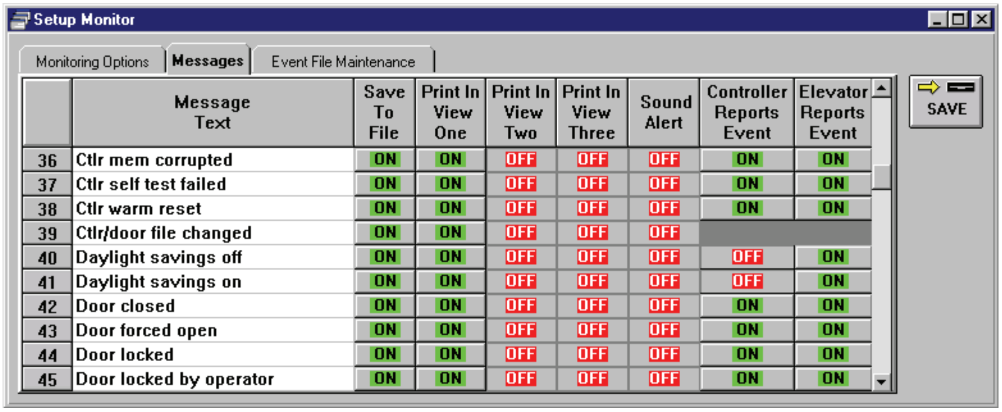
	Message Text	Save To File	Print In View One	Print In View Two	Print In View Three	Sound Alert	Controller Reports Event	Elevator Reports Event
1	Access by User ID denied	ON	ON	OFF	OFF	OFF	ON	ON
2	Access by User ID granted	ON	ON	OFF	OFF	OFF	ON	ON
3	Access denied	ON	ON	OFF	OFF	OFF	ON	ON
4	Access denied (access enable violation)	ON	ON	OFF	OFF	OFF	ON	ON
5	Access denied (access group violation)	ON	ON	OFF	OFF	OFF	ON	ON
6	Access denied (expiration violation)	ON	ON	OFF	OFF	OFF	ON	ON
7	Access denied (not in ctlr's user list)	ON	ON	OFF	OFF	OFF		
8	Access denied (pre-activation violation)	ON	ON	OFF	OFF	OFF	ON	ON
9	Access denied (reader locked out)	ON	ON	OFF	OFF	OFF	ON	ON
10	Access denied (secondary ID invalid)	ON	ON	OFF	OFF	OFF	ON	ON

Figure 5-8: Event Messages and Configuration Fields

3. Use the scroll bar on the right side of the window and scroll through the list of message texts until the "Daylight Savings Off" message text appears.
4. Scan across the row to the "Controller Reports Event" column and click in the cell. It will change from an ON button to an OFF button.
5. Locate the "Daylight Savings On" message text.
6. Scan across the row to the "Controller Reports Event" column and click in the cell. It will change from an ON button to an OFF button.

NOTE: The "Controller Reports Event" and "Elevator Reports Event" columns override all other columns. When either is turned "OFF", the event will not be reported regardless of what is selected in the other columns.

7. The messages tab window should look similar to Figure 5-9 on page 22 of this section.



	Message Text	Save To File	Print In View One	Print In View Two	Print In View Three	Sound Alert	Controller Reports Event	Elevator Reports Event
36	Ctlr mem corrupted	ON	ON	OFF	OFF	OFF	ON	ON
37	Ctlr self test failed	ON	ON	OFF	OFF	OFF	ON	ON
38	Ctlr warm reset	ON	ON	OFF	OFF	OFF	ON	ON
39	Ctlr/door file changed	ON	ON	OFF	OFF	OFF		
40	Daylight savings off	ON	ON	OFF	OFF	OFF	OFF	ON
41	Daylight savings on	ON	ON	OFF	OFF	OFF	OFF	ON
42	Door closed	ON	ON	OFF	OFF	OFF	ON	ON
43	Door forced open	ON	ON	OFF	OFF	OFF	ON	ON
44	Door locked	ON	ON	OFF	OFF	OFF	ON	ON
45	Door locked by operator	ON	ON	OFF	OFF	OFF	ON	ON

Figure 5-9: Controller Reports Event - After Changes

8. Click on the 

button. If the controller reports event change is not saved before clicking any other button or exiting the Setup Monitor window, the data entered is lost and must be re-entered.

9. Now update the access control network with the new information. Click on the 

button on the tool bar (for details on the update process refer to “Update the Network” on page 35 of this section).

1.2.6 Elevator Reports Events

When you have set up at least one door as an elevator, the elevator reports events fields allow an operator to filter out redundant elevator related events. This is due to the mechanism used to provide elevator control, where one reader is shared by the controllers at every elevator door on every floor.

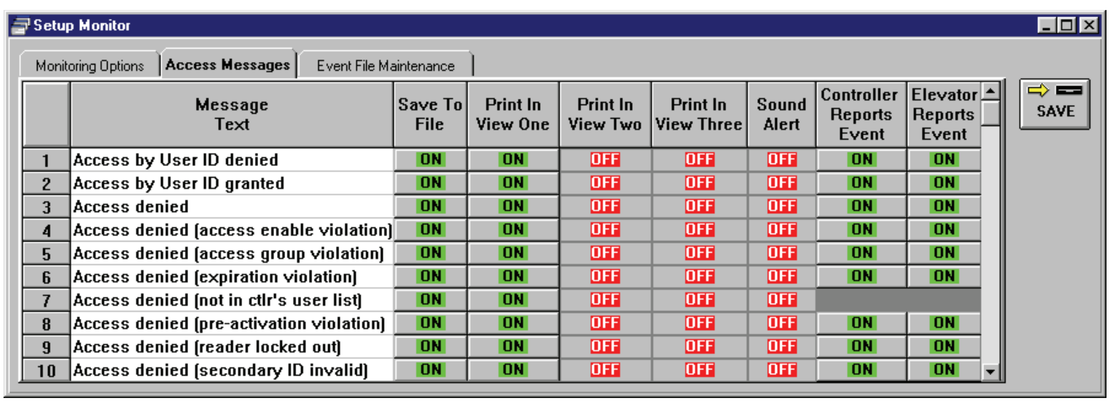
For example, eight controllers with eight elevator doors are wired to the one reader. The lock outputs for the eight controllers are connected to the elevator control hardware. A user presents a card to the reader. All eight controllers read the card and either allow or deny access depending on the user's access rights. If four controllers allow access and four controllers deny access, four "Access Granted" and four "Access Denied" messages are generated. This creates a lot of message traffic and takes up a lot of controller buffer space.

By using the elevator reports events field, you can disable these redundant messages only for those controllers configured for elevator control. The default is for all elevator control generated events to be stored and reported in the controller's event buffer.

NOTE: When a card is presented to a controller that is not recognized by the controller, the controller records an Unknown Key event message to the controller's event buffer. When the event buffer is downloaded to the host computer, the Doors program reviews the list of Unknown Key events and compares the card ID numbers to the user list. Any Unknown Key messages associated with card IDs that are in the user list are converted to Access Denied messages. This differentiates between cards that are truly "unknown" to the system from cards being presented by a user in an attempt to access an area in which the user is not allowed. In the elevator application, these event messages will be repeated by all controllers in the elevator network that do not recognize the card.

In this example, the message text string for "Access Denied" is disabled so it will not be stored and reported in the controller's event buffer.

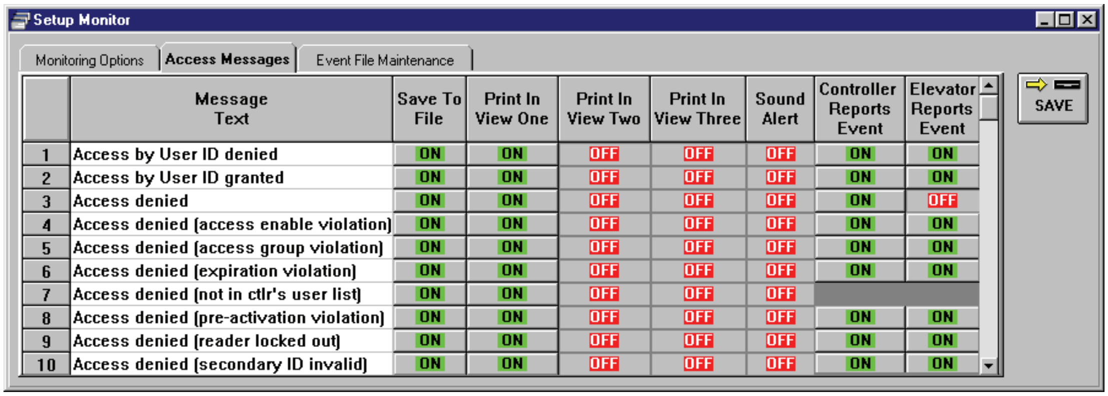
1. To access the message text strings, click on the Setup ⇒ Monitor and Events pull-down menu.
2. Click on the **Messages** tab. The Messages window appears (see Figure 5-10).



	Message Text	Save To File	Print In View One	Print In View Two	Print In View Three	Sound Alert	Controller Reports Event	Elevator Reports Event
1	Access by User ID denied	ON	ON	OFF	OFF	OFF	ON	ON
2	Access by User ID granted	ON	ON	OFF	OFF	OFF	ON	ON
3	Access denied	ON	ON	OFF	OFF	OFF	ON	ON
4	Access denied (access enable violation)	ON	ON	OFF	OFF	OFF	ON	ON
5	Access denied (access group violation)	ON	ON	OFF	OFF	OFF	ON	ON
6	Access denied (expiration violation)	ON	ON	OFF	OFF	OFF	ON	ON
7	Access denied (not in ctlr's user list)	ON	ON	OFF	OFF	OFF		
8	Access denied (pre-activation violation)	ON	ON	OFF	OFF	OFF	ON	ON
9	Access denied (reader locked out)	ON	ON	OFF	OFF	OFF	ON	ON
10	Access denied (secondary ID invalid)	ON	ON	OFF	OFF	OFF	ON	ON

Figure 5-10: Event Messages and Configuration Fields

3. Locate the "Access Denied" message text.
4. Scan across the row to the "Elevator Reports Event" column and click in the cell. It will change from an ON button to an OFF button.
5. The messages tab window should look similar to Figure 5-11 on page 24 of this section.



	Message Text	Save To File	Print In View One	Print In View Two	Print In View Three	Sound Alert	Controller Reports Event	Elevator Reports Event
1	Access by User ID denied	ON	ON	OFF	OFF	OFF	ON	ON
2	Access by User ID granted	ON	ON	OFF	OFF	OFF	ON	ON
3	Access denied	ON	ON	OFF	OFF	OFF	ON	OFF
4	Access denied (access enable violation)	ON	ON	OFF	OFF	OFF	ON	ON
5	Access denied (access group violation)	ON	ON	OFF	OFF	OFF	ON	ON
6	Access denied (expiration violation)	ON	ON	OFF	OFF	OFF	ON	ON
7	Access denied (not in ctlr's user list)	ON	ON	OFF	OFF	OFF		
8	Access denied (pre-activation violation)	ON	ON	OFF	OFF	OFF	ON	ON
9	Access denied (reader locked out)	ON	ON	OFF	OFF	OFF	ON	ON
10	Access denied (secondary ID invalid)	ON	ON	OFF	OFF	OFF	ON	ON

Figure 5-11: Elevator Reports Event - After Changes

NOTE: The "Controller Reports Event" and "Elevator Reports Event" columns override all other columns. When either is turned "OFF", the event will not be reported regardless of what is selected in the other columns.

6. Click on the 

button. If the controller reports event change is not saved before clicking any other button or exiting the Setup Monitor window, the data entered is lost and must be re-entered.

7. Now update the access control network with the new information. Click on the 

button on the tool bar (for details on the update process refer to "Update the Network" on page 35 of this section).

1.3 Saving and Archiving Event Files

There are two steps to saving and archiving event files.

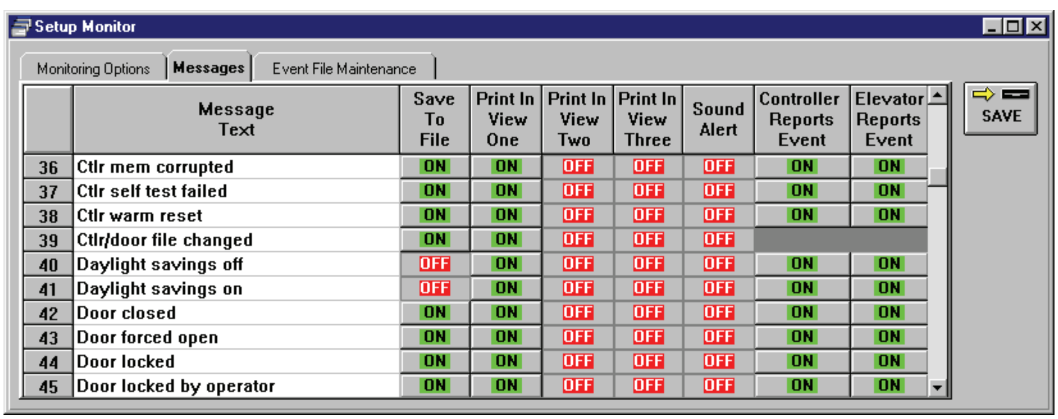
- save events to file on the host computer's hard disk
- archive files from the host computer's hard disk to a CD, floppy disk, or computer network.

1.3.1 Save to File

The save to file fields allow an operator to determine which events should be stored in the event file on the host computer's hard disk when events are uploaded from the controllers to the host computer. Many events are normal day to day activities that an operator may not want to have take up space on the hard disk. The default is for all events to be saved to the event file on the hard disk.

In this example, the message text strings notifying when the controllers enable/disable Daylight Savings time will be disabled so they will not be recorded to the event file on the host computer's hard disk.

1. To access the message text strings to not be saved to file, click on the Setup ⇒ Monitor and Events pull-down menu.
2. Click on the **Messages** tab. The Messages window appears (see Figure 5-11 on page 24 of this section).
3. Use the scroll bar on the right side of the window and scroll through the list of message texts until the "Daylight Savings Off" message text appears and scan across the row to the "Save To File" column.
4. Click in the cell. It will change from an ON button to an OFF button.
5. Locate the "Daylight Savings On" message text and scan across the row to the "Save To File" column.
6. Click in the cell. It will change from an ON button to an OFF button.
7. The messages tab window should look similar to Figure 5-12.



	Message Text	Save To File	Print In View One	Print In View Two	Print In View Three	Sound Alert	Controller Reports Event	Elevator Reports Event
36	Ctlr mem corrupted	ON	ON	OFF	OFF	OFF	ON	ON
37	Ctlr self test failed	ON	ON	OFF	OFF	OFF	ON	ON
38	Ctlr warm reset	ON	ON	OFF	OFF	OFF	ON	ON
39	Ctlr/door file changed	ON	ON	OFF	OFF	OFF		
40	Daylight savings off	OFF	ON	OFF	OFF	OFF	ON	ON
41	Daylight savings on	OFF	ON	OFF	OFF	OFF	ON	ON
42	Door closed	ON	ON	OFF	OFF	OFF	ON	ON
43	Door forced open	ON	ON	OFF	OFF	OFF	ON	ON
44	Door locked	ON	ON	OFF	OFF	OFF	ON	ON
45	Door locked by operator	ON	ON	OFF	OFF	OFF	ON	ON

Figure 5-12: Save to File - After Changes

8. Click on the SAVE button. If the save to file change is not saved before clicking any other button or exiting the Setup Monitor window, the data entered is lost and must be re-entered.

1.3.2 Archiving Old Events

The event files should be archived on a periodic basis. Archiving an event file, closes the original file and assigns it a descriptive name, allowing a new event file to be created. Periodic archiving prevents the event file from becoming too large for efficient data processing. Report generation can take a long time when the event files are too large. There are three event file archive types to select from.

- yearly (default setting)
- monthly
- weekly

1.3.2.1 Select Event File Type

1. To select the event file archive type, click on the Setup ⇒ Monitor and Events pull-down menu.
2. Click on the **Monitoring Options** tab. The Monitoring Options window appears (see Figure 5-13).

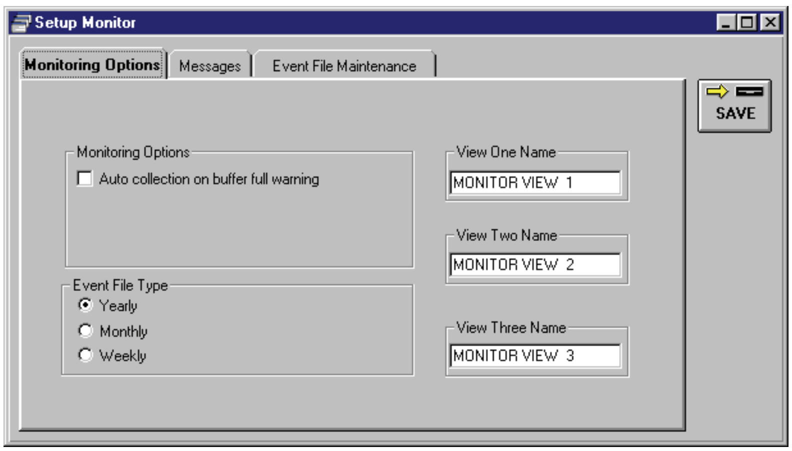


Figure 5-13: Monitoring Options Window

3. To select the event file type, click on the radio button next to your choice in the Event File Type field (see Figure 5-13). For this example verify the radio button next to the yearly option is selected.

NOTE: The default is set to archive yearly. Your selection of event file type will depend on the volume of events taking place. The more events you have, the more frequently you should archive. It is very important to pick a file type and stay with it. It is recommended you begin with yearly and only change to monthly or weekly if necessary. Once you have created an event file of a specific type, there is no way to change it.

4. Click on the  button. If the event file type change is not saved before clicking any other button or exiting the Setup Monitor window, the data entered is lost and must be re-entered.
5. An event file is automatically created. Click on the **Event File Maintenance** tab to see the created file (see Figure 5-14 on page 27 of this section).

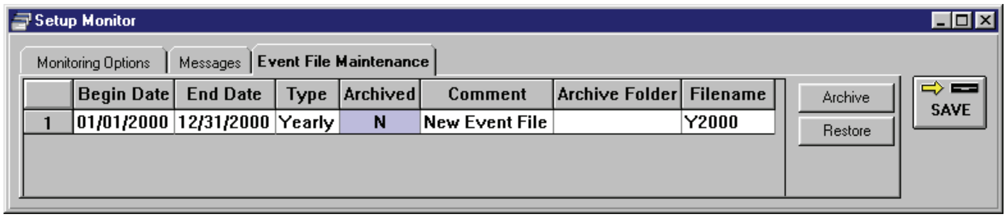


Figure 5-14: Event File Maintenance Window

NOTE: Once you have designated the file type you want to use, new files are automatically created at the beginning of each new period.

6. The Filename is automatically chosen depending on the file type you are using.

- yearly - YXXXX (where XXXX stands for the year - e.g. Y2000, Y2001, etc.).
- monthly - XXXYY (where XXX is an abbreviation for the month and YY is the last two digits of the year - e.g. AUG00, AUG01, etc.). Monthly is from the first to the last days of the month.
- weekly - WXXYY (where W stands for weekly and XX stands for the week of the year, 1-53 is used; YY is the last two digits of the year - e.g. W3800; W3801, etc.). Weekly is from Sunday through Saturday with no notice of the beginning or ending of a month.

1.3.2.2 Archiving Files

Once the end date of your file type has passed and a new event file has been automatically created, you are ready to archive the old file.

NOTE: Before you archive a file, set up a folder where you plan to store the archived files on the host computer. The destination of the archive should not be the Doors directory to avoid confusion. Be sure to name it something that will be easy to identify and locate.

1. To archive the file, click on the Setup ⇒ Monitor and Events pull-down menu.
2. Select the **Event File Maintenance** tab.
3. Click on the file to be archived. The window should appear similar to Figure 5-15.

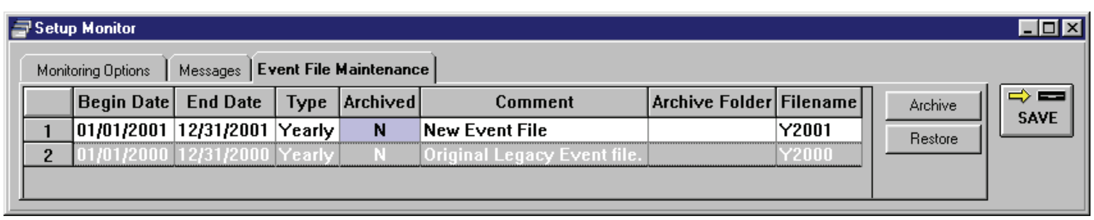


Figure 5-15: Event File Maintenance Window - Ready To Archive

4. Click on the  button. The Select Folder for Archive File window will appear (see Figure 5-16).

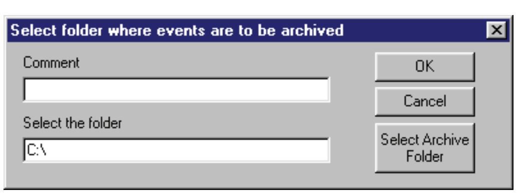


Figure 5-16: Select Folder For Archive File Window

5. Click on the 

button. The Browse for Archive Folder window will appear. Select the folder you have previously set up for the archives (see Figure 5-17).

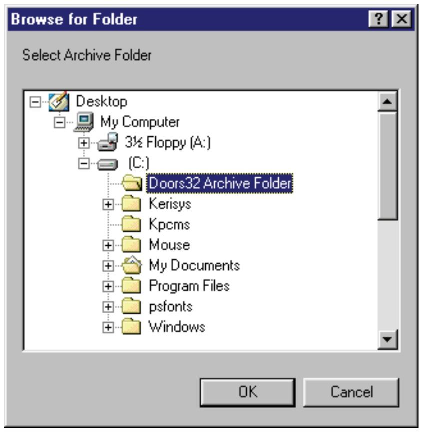


Figure 5-17: Browse for Archive Folder Window

6. Click on the 

button. The Selected Folder for Archive File window will appear (see Figure 5-18).

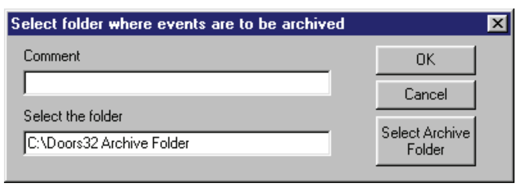


Figure 5-18: Selected Folder for Archive File Window

NOTE: The Comment field may be used by the operator to describe what events are included in the file.

7. Click on the 

button. The Event File Maintenance window should look similar to Figure 5-19.

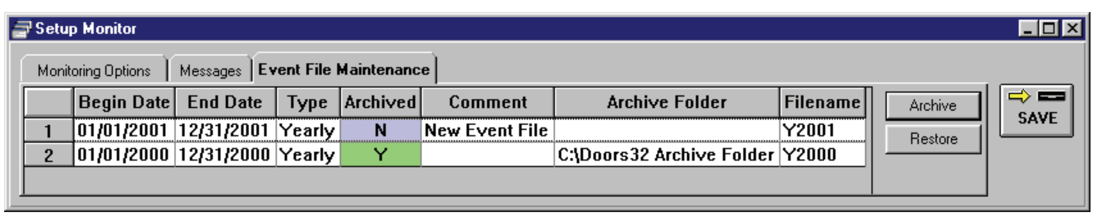


Figure 5-19: Completed Archive

1.3.2.3 Restoring Archived Files

If you need to search events further back in history than the current file, you will need to restore the necessary file.

1. To restore archived files, click on the Setup ⇒ Monitor and Events pull-down menu.
2. Click on the **Event File Maintenance** tab. The Event File Maintenance window appears.
3. Click on the file to be restored. The window should appear similar to Figure 5-20.

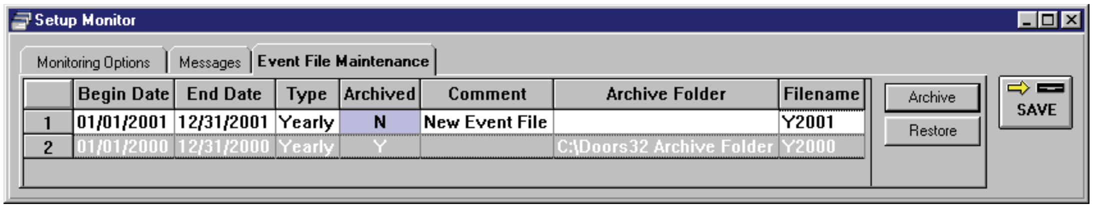


Figure 5-20: Event File Maintenance Window with Archived File

4. Click on the 

button. The Select Folder for Restore window will appear. Select the folder where the archived files have been placed previously (see Figure 5-21).

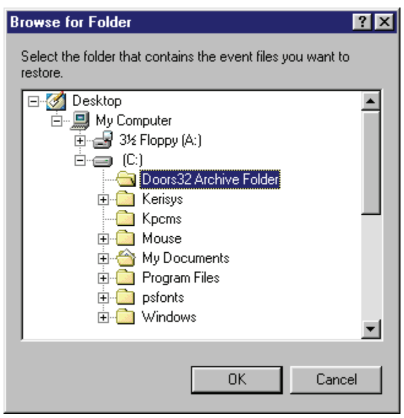


Figure 5-21: Select Folder for Restore

5. Click on the 

button. The Event File Maintenance window will appear again (see Figure 5-22).

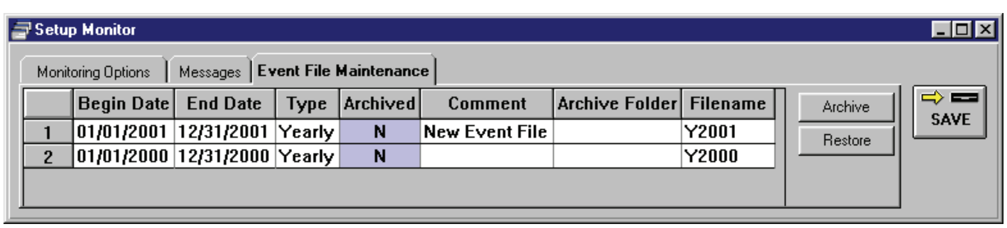


Figure 5-22: Restored Event File

6. The archived file has now been restored and is available for searching.

NOTE: Once you have finished using the restored files, you will need to return them to the archive folder by repeating the archiving steps shown in "Archiving Files" on page 27 of this section.

1.4 Auto Deletion of Archived Event Files

Using the Windows Scheduled Task program, Doors events may be scheduled for auto deletion.

1. Click the  button. A pop-up menu of commands appears.

2. Click the **Control Panel** menu option. The Control Panel window appears (see Figure 5-23).

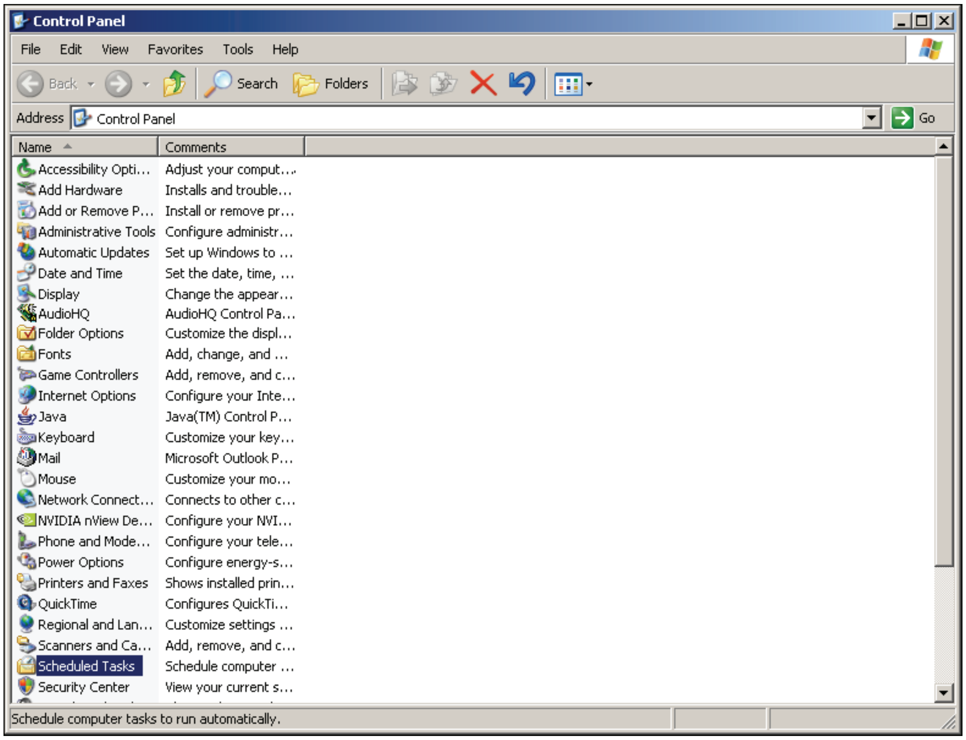


Figure 5-23: Control Panel Window

3. Double-click on the **Scheduled Task** option. The Scheduled Task window appears (see Figure 5-24).

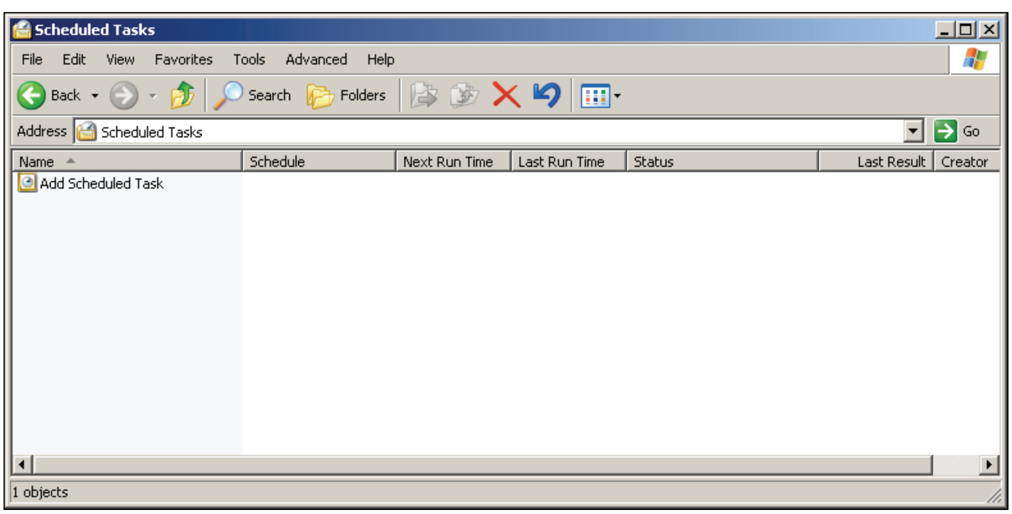


Figure 5-24: Scheduled Tasks Window

4. Double-click on the **Add Scheduled Task** option. The Scheduled Task Wizard window will appear (see Figure 5-25).

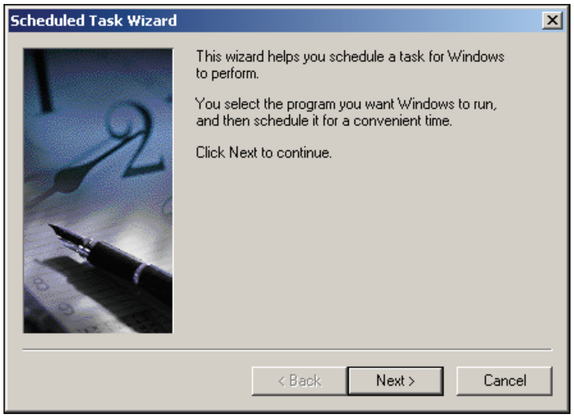


Figure 5-25: Scheduled Task Wizard - Opening Window

5. Click on the Next > button.The next window in the Scheduled Task Wizard will appear (see Figure 5-26).



Figure 5-26: Scheduled Task Wizard - Locate Program

6. Click on the Browse... button.The next window in the Select Program To Schedule window will appear (see Figure 5-27 on page 32 of this section).

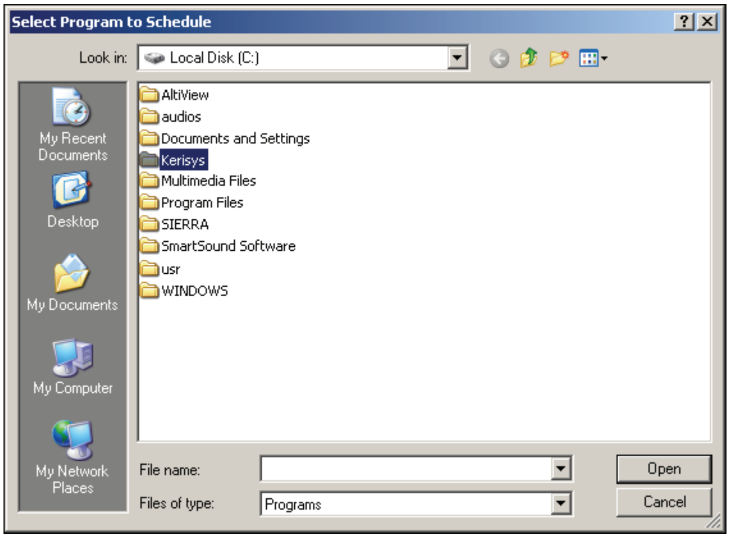


Figure 5-27: Select Program to Schedule

7. Select Kerisys, then click on the Open button (or double-click on the **Kerisys** option). The Kerisys folder will open (see Figure 5-28).

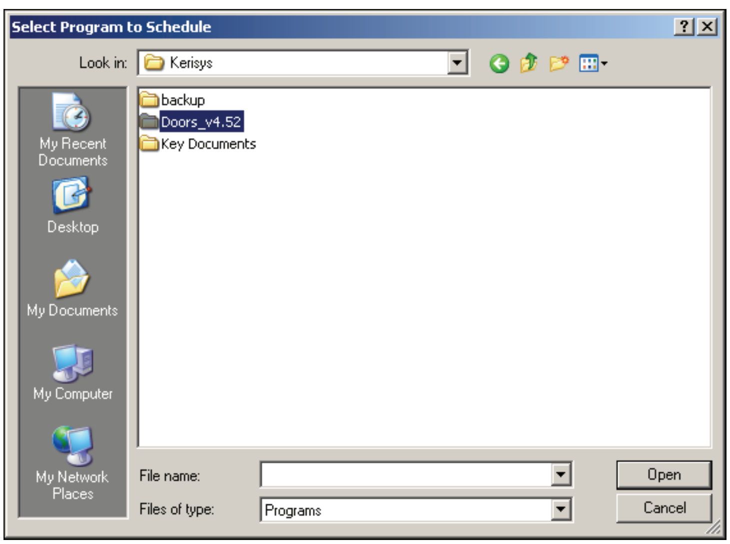


Figure 5-28: Select Program to Schedule - Kerisys Folder

8. Select the current version of Doors installed on the PC, then click on the Open button (or double-click on the current version of Doors). The next window will open (see Figure 5-29 on page 33 of this section).

NOTE: Make sure to select the current version of Doors installed on the PC.

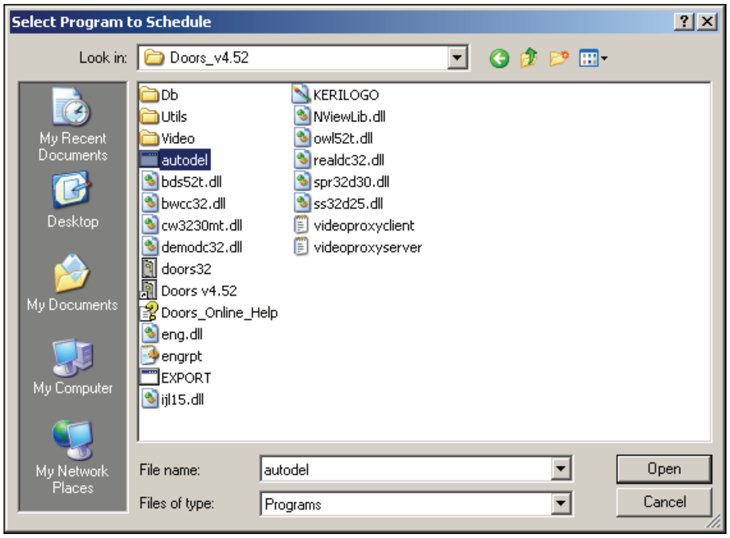


Figure 5-29: Select Autodel Program to Schedule

9. Select the autodel.exe option, then click on the  button (or double-click on the autodel.exe option). The next window will open (see Figure 5-30).



Figure 5-30: Name and Select the Frequency of Auto Delete

10. There is the option to give this auto delete progam a specific name. Choose a name that will be easy to remember, for example, DoorsAutoDelete.
11. Select the frequency of the auto delete task, by clicking in one of the radio buttons nect to the desired option. Click on the  button.

12. Depending on the frequency selected, different windows will appear showing many different options. Select the various options for how the auto delete program should perform the deletion task. When all options have been selected, click on the  button until the User Name and Password window appears (see Figure 5-31 on page 34 of this section).

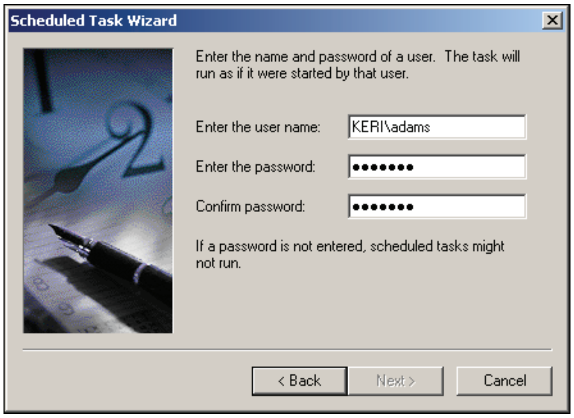


Figure 5-31: Enter Name and Password

13. Enter a user name along with their password in the fields provided. The scheduled auto deletion will be carried out as if it were started by this user. When the information has been entered, click on the Next > button, followed by the Finish button.

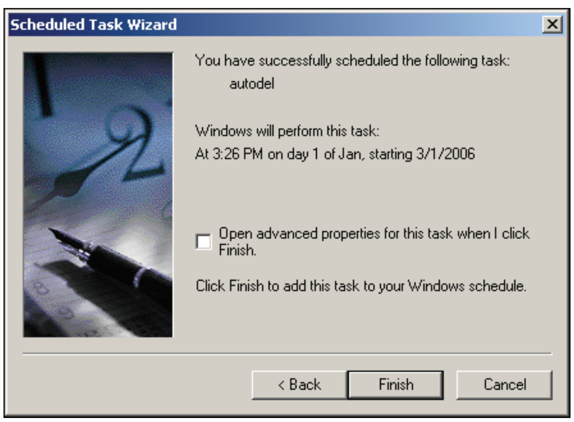


Figure 5-32: Auto Delete Confirmed

14. The auto delete schedule now appears in the Scheduled Tasks window (see Figure 5-33).

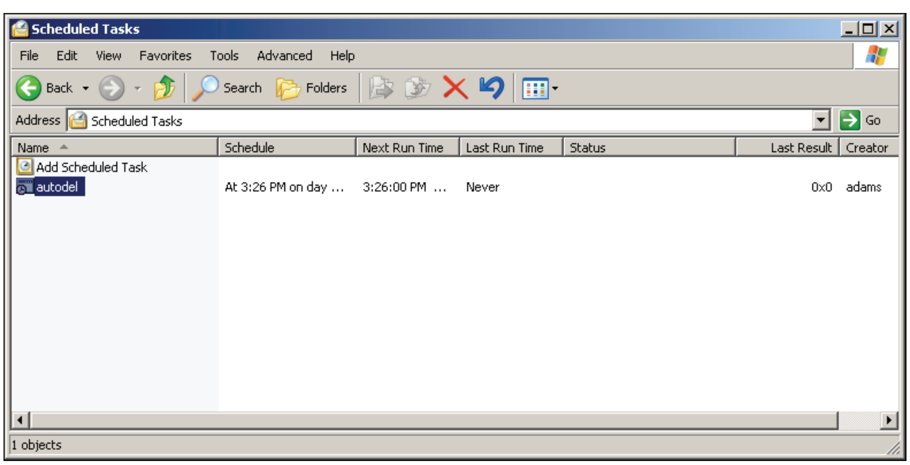


Figure 5-33: Auto Delete Schedule Complete

2.0 Update and Collect Events from the Controllers

Now that all of the instructions necessary for day-to-day operation of the access control network have been entered, they must be downloaded to the access control network.

2.1 Update the Network

The Update Network commands uploads from the host computer to the access control network any changes made to the *Doors* databases.

1. Click on the 

icon on the tool bar. The Update Network window will appear. If changes have been made and the network needs to be updated, the Update Required field will indicate this with a “Yes”, and the Skip/Update toggle box under the Smart Update Network field will indicate “Update” (see Figure 5-34).

*NOTE: The Smart Update Network command uploads from the host computer to the access control network **only** the changes made to the Doors databases since the last update was performed. While setting up the databases and at most times in the future, using the Smart Update will meet your needs. There may be times, however, when you want to re-send **all** database information to the controllers. In such cases, click on the Skip/Update toggle box under the Total Update Network field and the word “Skip” will toggle to “Update”.*

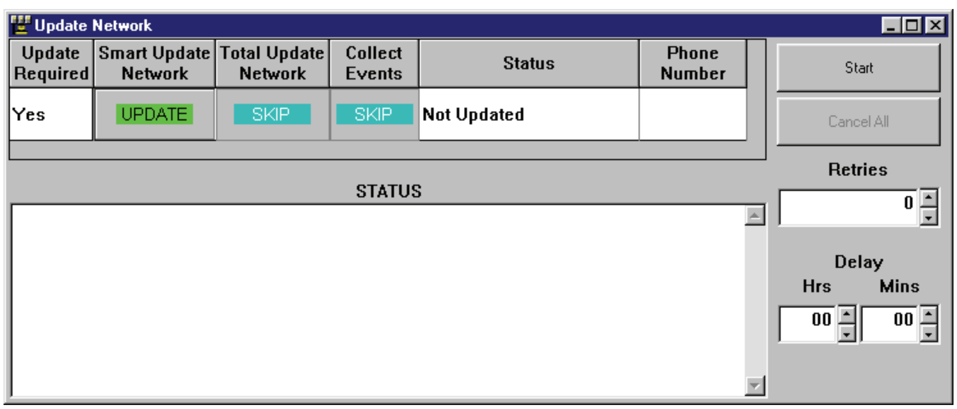


Figure 5-34: Required Network Update

2. Click on the 

button to begin Update of the Network.

NOTE: Click on the 

button at any time to stop the update process.

3. Once all parameters are collected, the host computer connects to the access control network (if it isn’t already connected). The Net Communication window appears if the access control network connection needs to be made (see Figure 5-35 on page 36 of this section).

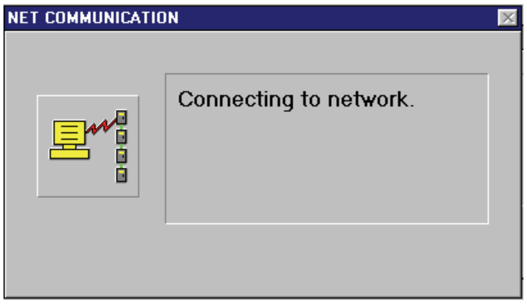


Figure 5-35: Connecting to the Network

4. Once the connection is made, the progress of the update may be viewed through the Status windows. The status windows will indicate when the update is complete (see Figure 5-36).

NOTE: Once the update process has begun, please be patient. The update process can take anywhere from several seconds to several minutes depending upon the amount of information to be updated and the number of controllers receiving information.

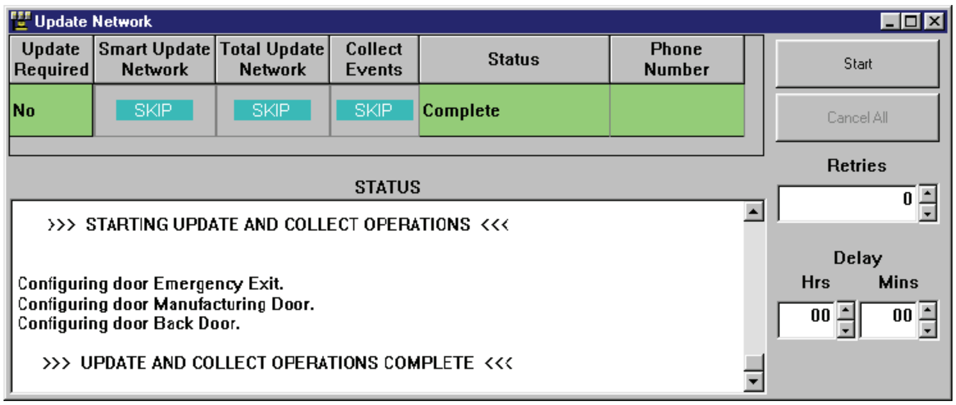


Figure 5-36: Successful Network Update

5. The access control network has now received all new default operating parameters and is ready for basic operation.

2.1.1 Delaying the Network Update

If you would like the host computer to wait for a period of time until it uploads the new information to the controllers, you may delay the start time of the update.

1. In the Update Delay field, use the spinners to select how long you want the host computer to wait until it begins updating the network. For this example we will enter 1 minute (see Figure 5-37). This means that the host computer will wait for 1 minute until it begins to update the network.



Figure 5-37: Update Delay

2. If there is a possibility the host computer will be unable to connect with the controllers, you may indicate how many times the system should attempt a connection before canceling the update. Use the spinner icons in the Retries field to select the number of attempts.

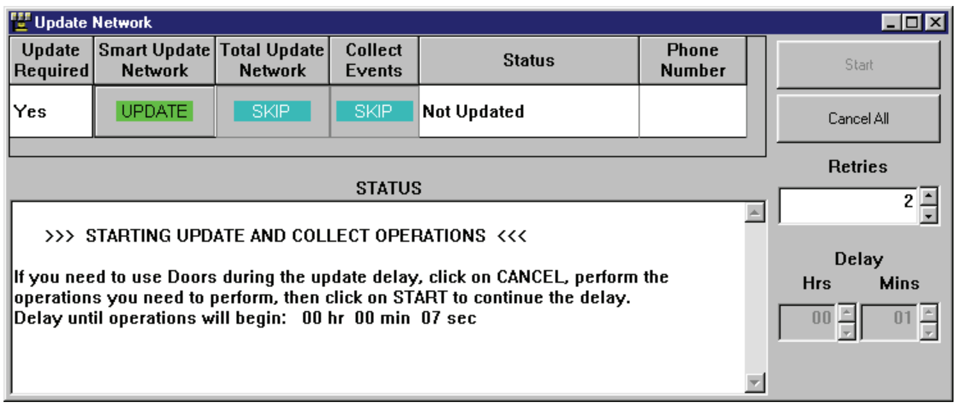


Figure 5-38: Delay Countdown Window

3. Click on the  button to begin the countdown until the update operation will begin. The progress of the countdown may be viewed through the Status windows (see Figure 5-38).

NOTE: While the host computer is waiting to upload to the network, you will not be able to use or close Doors. You will not be allowed to properly shut down the host computer. You may cancel the countdown at any time to use the system and resume the countdown when you are ready. When you resume, the countdown will continue from the last full minute where it left off.

2.2 Collecting Events While Updating

Collecting events from all controllers clears the controller buffers and stores the events in an event file on the hard disk. Event data can then be processed into report formats. Updating the network and collection of events data may be performed at the same time.

1. Click on the 

icon on the tool bar. The Update Network window will appear. Click on the Skip/Update toggle box under Collect Events. The word "Skip" will be toggled to "Collect" (see Figure 5-39).

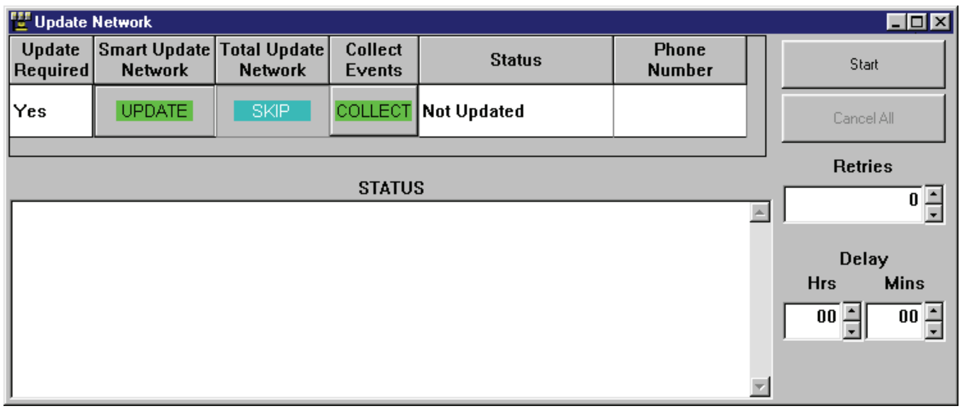


Figure 5-39: Collect Events

2. Click on the 

button to begin collecting events data from the network.
3. The host computer connects to the access control network (if it isn't already connected). The Network Communication window appears if the access control network connection needs to be made (see Figure 5-40).

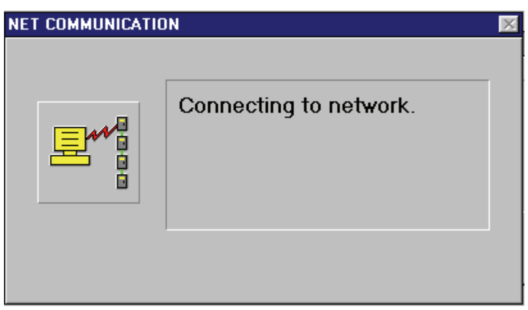


Figure 5-40: Connecting to the Network

4. Once the connection is made, the progress of the event collection may be viewed through the Status windows. The status windows will indicate when the event collection is complete (see Figure 5-41 on page 39 of this section).

NOTE: Once the event collection process has begun, please be patient. The collection process can take anywhere from several seconds to several minutes depending upon the amount of information to be collected and the number of controllers sending information.

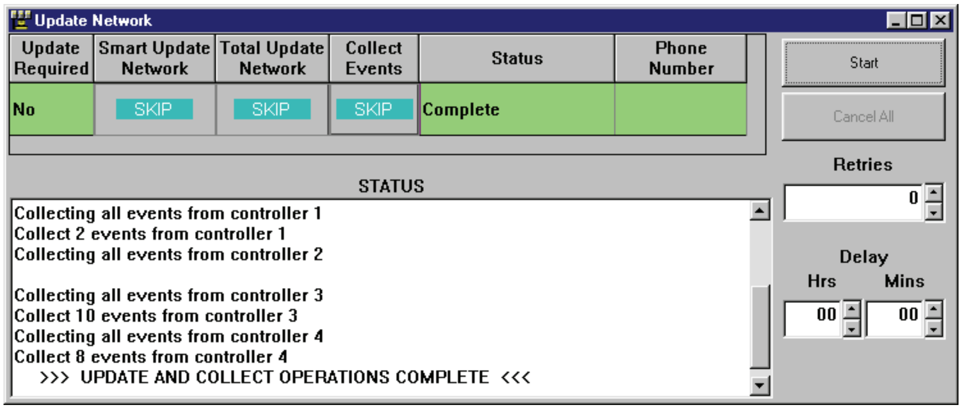


Figure 5-41: Successful Collection of Events from Network

5. The host computer has now collected all events data from the access control network and is ready to be processed into report format (see "Reporting" on page 1 in section 7).

3.0 Monitor and Collect Events from the Controllers

This section describes the use of the monitor windows and the process for collecting events from all controllers on the access control network for storage on the host computer's hard disk.

1. To enter the Operate Monitor window, click on the Operate ⇒ Start Monitor pull-down menu or click on the  icon on the tool bar. The Operate Monitor window appears (see Figure 5-42).

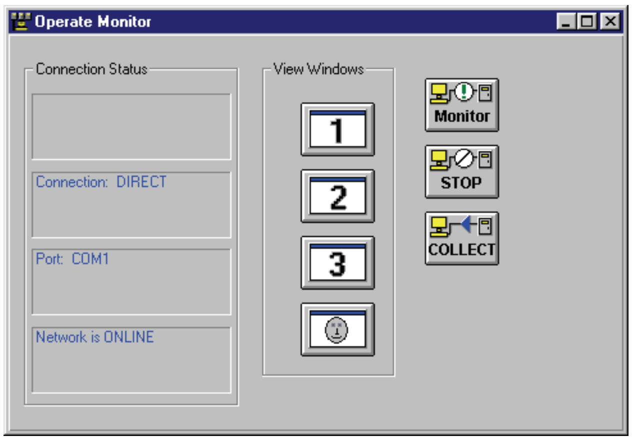


Figure 5-42: Operate Monitor Window

NOTE: Sound Alerts are only active when Doors is in monitor mode. For more information about sound alerts, refer to "Sound Alert on Event" on page 19 of this section.

3.1 Verifying Communication Status

The Connection Status field displays the communication connection status between host computer and access control network. Within the connection status field four panes with information (see Figure 5-42). From top to bottom:

- Pane 1 (at the top) displays event collection status when event collection is underway – the number of events collected from each controller and the number of events processed by a monitor window.
- Pane 2 (second from the top) displays the type of connection between host computer and access control network – direct using a cable between master controller and host computer or remote using modems between master controller and host computer.
- Pane 3 (third from the top) displays the COM port used for communication.
- Pane 4 (at the bottom) displays if the network is ONLINE (actively connected and communicating with the host computer) or OFFLINE (disconnected from the host computer).

3.2 Starting Monitoring

The view window field is made up of three buttons: , , and ; one for each monitoring window (see Figure 5-42 on page 40 of this section).

1. To open a monitor window, click on the button corresponding to the desired monitor.

NOTE: Before opening a monitor, it must have been set up in the Setup ⇒ Monitors and Events section, defining what it monitors. Otherwise, the default is for monitor one to view all events, and for monitors two and three to view no events. See "Setup Monitor Windows and Events" on page 3 of this section.

2. Once a monitor window is open, an operator can size it according to how the operator wants the monitor window positioned on the *Doors* window.
3. Any combination of the three monitor windows can be open at the same time. Each can be sized individually, but the default is for all three windows to be tiled horizontally across the *Doors* window (see Figure 5-43).

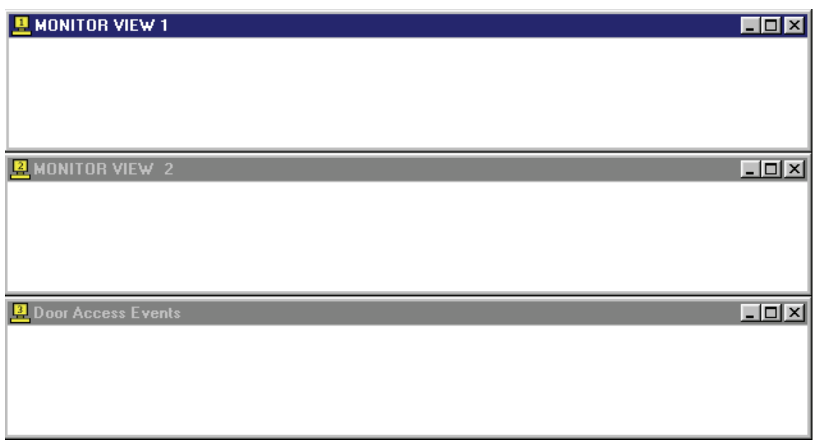


Figure 5-43: Tiled Monitoring Windows

4. Once monitoring windows have been opened, monitoring can begin. Click on the  button. If communication has not been established between the host computer and the access control network, *Doors* will make the connection.
5. As events occur on the access control network that meet the criteria of the monitoring window, they will be displayed in the monitoring window.

3.3 Display Photo While Monitoring

The Display Photo feature is designed to allow the operator to see the photos associated with each user as they attempt to gain access through the master controller's A-reader. Display Photo makes it easier for an operator monitoring activity on the master controller to see exactly who it is attempting access without having to open the Show Photo in the Setup Users window.

NOTE: Badging must be enabled (but does not need to have a license code) and a photo must be associated with the user in order for it to appear in the Photo View window. For further information on how to enable badging and associate a photo with the user, see "Enable Badging in Doors" on page 15 in section 9 and "Acquire and Edit User Photo" on page 20 in section 9.

1. From the Operate Monitor window (see Figure 5-42 on page 40 of this section), click on the 

button. If communication has not been established between the host computer and the access control network, *Doors* will make the connection.
2. Click on the  button. The Photo View window will appear (see Figure 5-44).

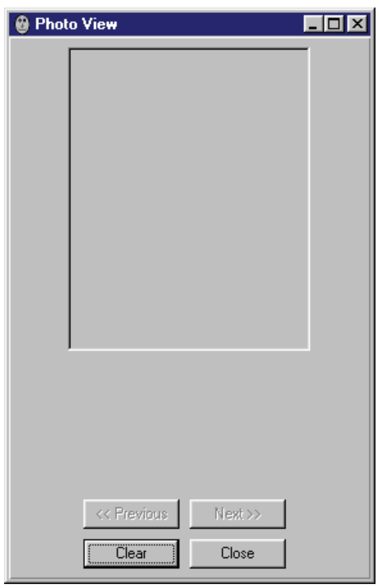


Figure 5-44: Photo View Window

3. Once the Photo View window is open, an operator can size it according to how the operator wants it positioned on the *Doors* window. Any combination of the Photo View and the three monitor windows can be open at the same time. Each can be sized individually.
4. As a user attempts to gain access to the master controller, the photo associated with that user will appear in the Photo View window (see Figure 5-45 on page 43 of this section).

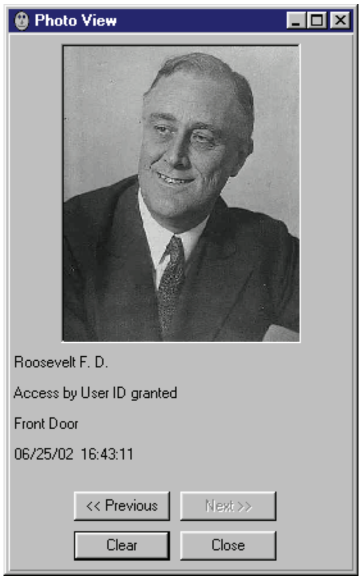


Figure 5-45: Photo View Window With Photo

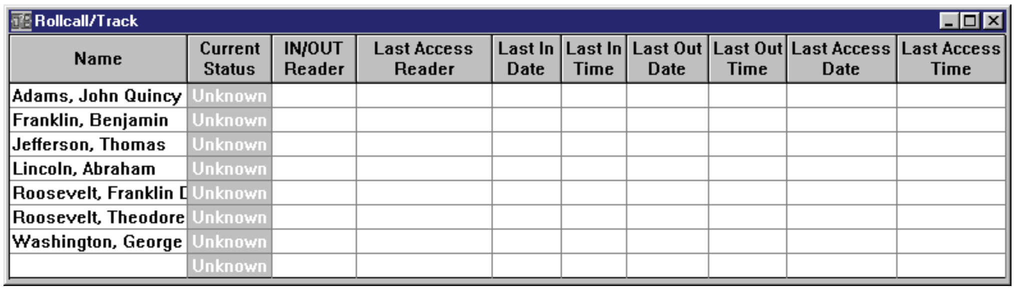
5. The Photo View window displays the following information:
   - user name
   - access status
   - door accessed
   - date and time of attempt

3.4 Rollcall/Track

The Rollcall/Track feature allows the operator to monitor user status in a spreadsheet format. To designate which users should appear on the Rollcall/Track listing see “Setup Users” on page 1 in section 4.

NOTE: Rollcall/Track information is automatically updated only when you are in monitor mode (see “Starting Monitoring” on page 41 of this section).

1. To enter the Rollcall/Track window while in monitoring mode, click on the Operate ⇒ Rollcall/Track pull-down menu. The Rollcall/Track window appears (see Figure 5-46).



Rollcall/Track

Name	Current Status	IN/OUT Reader	Last Access Reader	Last In Date	Last In Time	Last Out Date	Last Out Time	Last Access Date	Last Access Time
Adams, John Quincy	Unknown								
Franklin, Benjamin	Unknown								
Jefferson, Thomas	Unknown								
Lincoln, Abraham	Unknown								
Roosevelt, Franklin D	Unknown								
Roosevelt, Theodore	Unknown								
Washington, George	Unknown								
	Unknown								

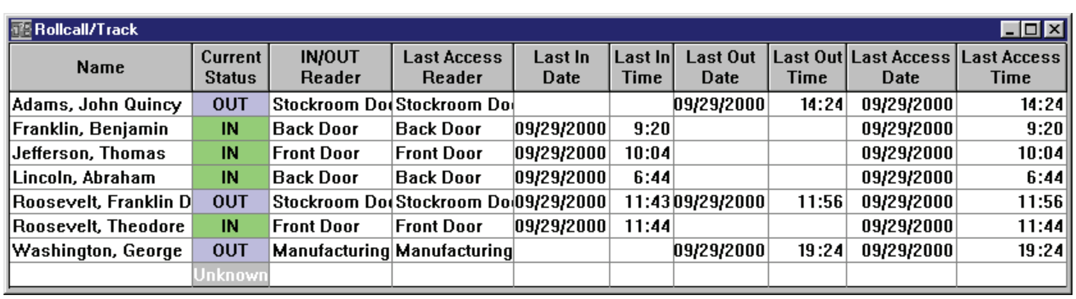
Figure 5-46: Rollcall/Track Window

2. As the users gain access through a door, the event information of that access is automatically updated on the Rollcall/Track window (see Figure 5-47).

The following information is provided in the Rollcall/Track window:

Name – user name
Current Status – reader type-usage (i.e. standard, in, out, or muster) of last door accessed
In/Out Reader – last access of a door designated as in, out, or muster
Last Access Reader – last door accessed
Last In Date/Time – last access of a door assigned a reader type-usage of IN
Last Out Date/Time – last access of a door assigned a reader type-usage of OUT
Last Access Date/Time – last access of any door

NOTE: Access granted through an EntraGuard unit by a User ID does not appear in the Rollcall/Track window.



Rollcall/Track

Name	Current Status	IN/OUT Reader	Last Access Reader	Last In Date	Last In Time	Last Out Date	Last Out Time	Last Access Date	Last Access Time
Adams, John Quincy	OUT	Stockroom Do	Stockroom Do			09/29/2000	14:24	09/29/2000	14:24
Franklin, Benjamin	IN	Back Door	Back Door	09/29/2000	9:20			09/29/2000	9:20
Jefferson, Thomas	IN	Front Door	Front Door	09/29/2000	10:04			09/29/2000	10:04
Lincoln, Abraham	IN	Back Door	Back Door	09/29/2000	6:44			09/29/2000	6:44
Roosevelt, Franklin D	OUT	Stockroom Do	Stockroom Do	09/29/2000	11:43	09/29/2000	11:56	09/29/2000	11:56
Roosevelt, Theodore	IN	Front Door	Front Door	09/29/2000	11:44			09/29/2000	11:44
Washington, George	OUT	Manufacturing	Manufacturing			09/29/2000	19:24	09/29/2000	19:24
	Unknown								

Figure 5-47: Rollcall/Track Window with Events

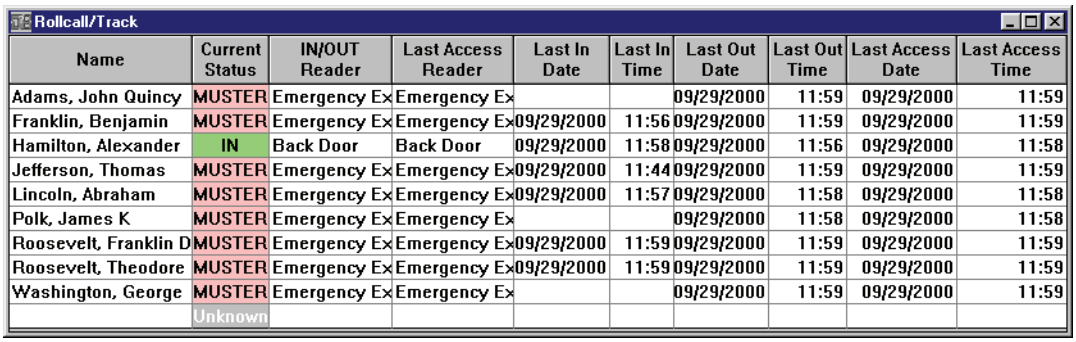
NOTE: The cells will be filled according to how the individual doors were configured (see “Door Configuration” on page 26 in section 3).

3.4.1 Muster Reader

One reader may be designated as a Muster reader (see “Assign a Reader Type (Usage)” on page 30 in section 3). In the event of an emergency, as each user presents their card to the Muster reader, the operator will be able to tell immediately which users are accounted for and the last door accessed by those who are unaccounted for.

NOTE: Rollcall/Track information is automatically updated only when you are in monitor mode (see “Starting Monitoring” on page 41 of this section).

1. Once one card has been presented to the Muster reader, ALL users will appear on the Rollcall/Track window, including those who have the Rollcall/Track feature disabled on their card (see “Entering User Data – Dialog Box Method” on page 13 or page 22 in section 4). The users who have the Rollcall/Track disabled on their card will remain on the Rollcall/Track listing until the window is closed and reopened.



Name	Current Status	IN/OUT Reader	Last Access Reader	Last In Date	Last In Time	Last Out Date	Last Out Time	Last Access Date	Last Access Time
Adams, John Quincy	MUSTER	Emergency Ex	Emergency Ex			09/29/2000	11:59	09/29/2000	11:59
Franklin, Benjamin	MUSTER	Emergency Ex	Emergency Ex	09/29/2000	11:56	09/29/2000	11:59	09/29/2000	11:59
Hamilton, Alexander	IN	Back Door	Back Door	09/29/2000	11:58	09/29/2000	11:56	09/29/2000	11:58
Jefferson, Thomas	MUSTER	Emergency Ex	Emergency Ex	09/29/2000	11:44	09/29/2000	11:59	09/29/2000	11:59
Lincoln, Abraham	MUSTER	Emergency Ex	Emergency Ex	09/29/2000	11:57	09/29/2000	11:58	09/29/2000	11:58
Polk, James K	MUSTER	Emergency Ex	Emergency Ex			09/29/2000	11:58	09/29/2000	11:58
Roosevelt, Franklin D	MUSTER	Emergency Ex	Emergency Ex	09/29/2000	11:59	09/29/2000	11:59	09/29/2000	11:59
Roosevelt, Theodore	MUSTER	Emergency Ex	Emergency Ex	09/29/2000	11:59	09/29/2000	11:59	09/29/2000	11:59
Washington, George	MUSTER	Emergency Ex	Emergency Ex			09/29/2000	11:59	09/29/2000	11:59
	Unknown								

Figure 5-48: Rollcall/Track Window in Muster Mode

NOTE: EntraGuard units are not able to act as a Muster reader and access granted through an EntraGuard unit with a User ID does not appear in the Rollcall/Track window.

3.5 Collecting Events While Monitoring

Collecting events from all controllers clears the controller buffers and stores the events in an event file on the hard disk. Event data can then be processed into report formats. Collection of events occurs when you start monitoring and continues while monitoring.

1. To collect events, click on the  button. If communication has not been established between the host computer and the access control network, *Doors* will make the connection.
2. Pane 1 in the communication status field will display event collection status as each controller is contacted (see Figure 5-42 on page 40 of this section). When complete, Pane 1 will go blank.

3.6 Acknowledging Sound Alerts

When an event that generates a sound alert occurs, the Windows Exclamation sound or PC speaker beep is played repeatedly until acknowledged by the operator.

1. When there is a sound alert to be acknowledged, the sound alert button on the tool bar changes from  to  and the Windows Exclamation sound or PC speaker beep is played repeatedly.

   To acknowledge the sound alert click on the  button. The alarm is acknowledged and the button changes back to .

NOTE: If the sound alert button is in the  *state, but the Windows Exclamation sound or PC beep is playing, the Exclamation sound has been generated by another program operating under Windows and is **not** an alarm event. If the sound alert button is in the*  *state, but the Windows Exclamation sound or PC beep is not playing, there **is** a sound alert to be acknowledged and this indicates there is a problem with the host computer's ability to generate a sound.*

3.7 Stopping Monitoring

There are two ways to stop the monitoring process.

1. Click on the  button in the Operate Monitor window (see Figure 5-42 on page 40 of this section). This ends the monitoring process but does not close the monitoring windows or the communication link between host computer and access control network.
2. To close all system monitor windows and disconnect the host computer from the access control network, click on the Operate ⇒ Stop Monitor pull-down menu or click on the  icon on the tool bar.

4.0 System Maintenance

To provide the best long-term operating conditions for the *Doors* software, there are two system maintenance steps that should be performed.

- secure storage of the *Doors* program CD-ROM
- periodic backup of the *Doors* software

4.1 Secure Storage of Program CD-ROM

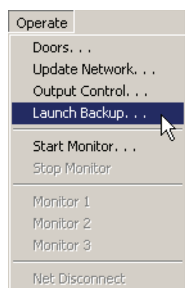
The original *Doors* installation CD-ROM should be stored in a safe, secure place away from environmental extremes. Safe, secure storage is not just for the sake of software reinstallation should there be a host computer system crash, but to keep the software out of the hands of unauthorized personnel.

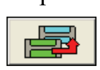
Using the installation CD-ROM, it is possible for an unauthorized person to reinstall the *Doors* software and use the default passwords to modify the system operator database. This can result in the creation of an operator or user that will have unlimited access to the secured area, violating the integrity of the access control system.

4.2 Periodic Software Backup

The *Doors* access control software and its databases should be backed-up periodically. The more often the system is backed-up, the less data reconstruction will need to be done in the event of a host computer system crash. Beginning with *Doors* v4.30 a backup tool (Abakt) has been built into the *Doors* program.

The backup tool is automatically installed with *Doors* and may be launched 3 different ways.

- From within *Doors* using the drop-down menu 

- From within *Doors* using the  button
- Independent of the Doors program

4.2.1 Configure Abakt

There are four main sections in Abakt.

Source Page - select and add directories to be backed up.
Filters Page - files to be backed up are added or excluded.
Backup Type Page - select backup type

- Create New - never overwrite existing backup with the same file name
- Replace Existing - replace existing backup with the same filename
- Update Existing - add new files and update existing files already present in existing backup with the same file name
- Freshen Existing - update files already present, don't add new files to existing backup with the same file name

Destination Page - select the file name and location for the backup file

The following is a few basic instructions for using Abakt to back up the *Doors* installation. For further information, refer to the Abakt program's Help.

1. To launch Abakt, click on the Operate ⇒ Launch Backup pull-down menu or click on the  tool bar button.

NOTE: To prevent potential file access errors, the Doors program must be closed before the files and databases can be backed up.

2. A Launch Backup confirmation window appears (see Figure 5-49).

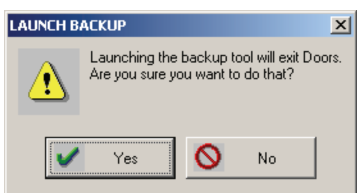
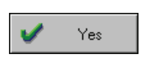


Figure 5-49: Launch Backup Confirmation

3. To keep *Doors* running and not launch Abakt, click on the 

button.
4. To close *Doors* and launch Abakt, click on the 

button.
5. *Doors* will close and the backup program will open (see Figure 5-50 on page 49 of this section).

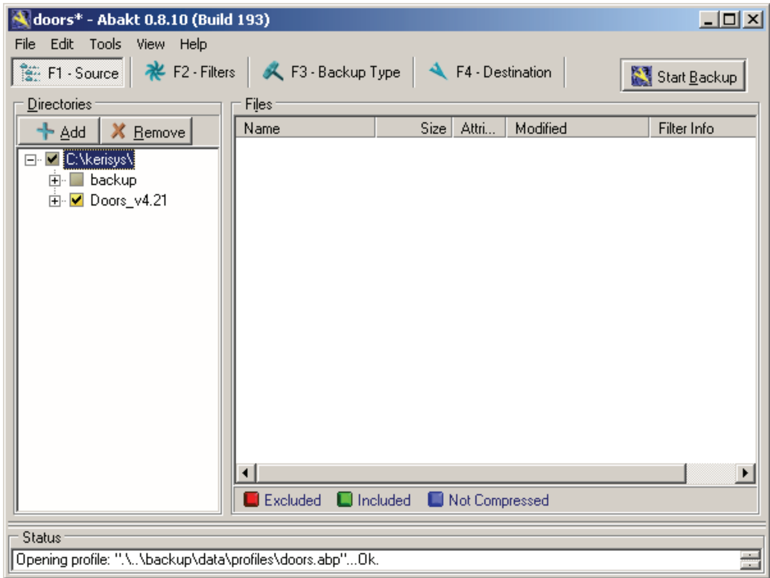


Figure 5-50: Abakt Window

NOTE: Make sure no other workstations are accessing the Doors database files when performing a backup. Failure to do so may result in some files being skipped and therefore not being backed-up.

4.2.1.1 Setup Source

The default location that will be backed up is found at C:\kerisys\. If *Doors* was installed in a directory other than the default, the profile must be updated.

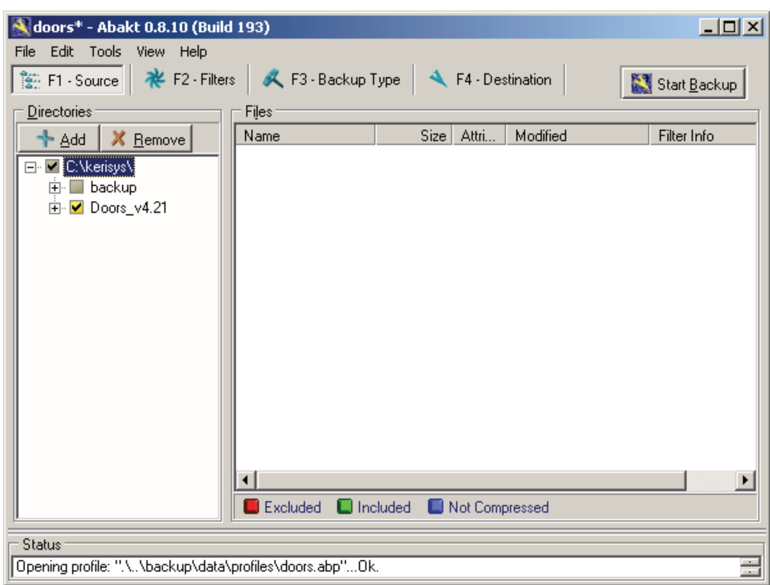
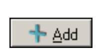


Figure 5-51: Abakt - Setup Source Page

1. To change the location of the files to be backed up, click on the 

button. A Browse for Folder window appears (see Figure 5-51 on page 49 of this section).

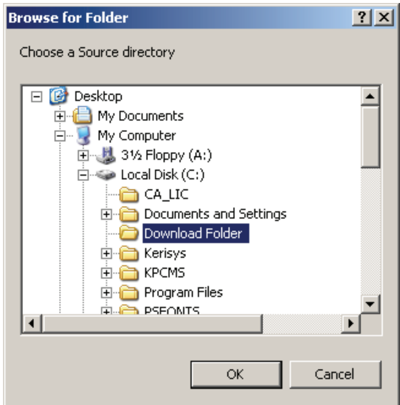


Figure 5-52: Browse for Folder Window

2. Locate the folder where the *Doors* database is located and click on the  button.
3. The new location is shown in the “Directories” field (see Figure 5-53).

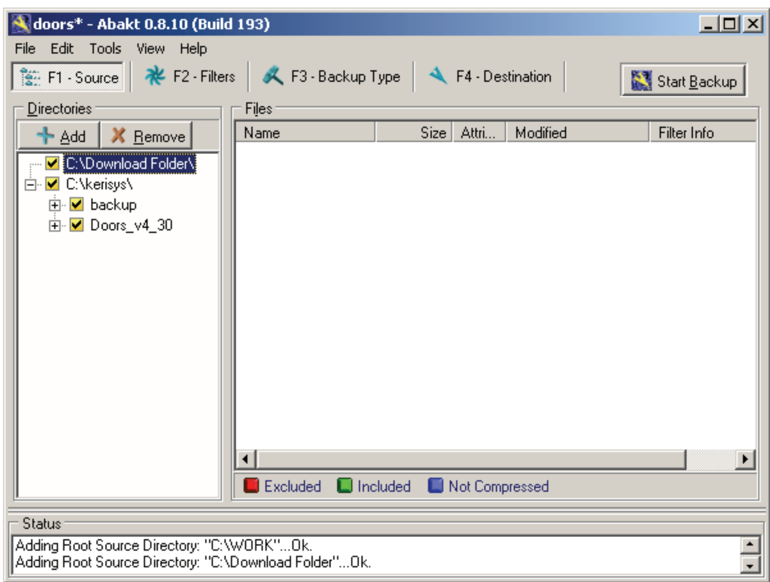


Figure 5-53: New Source for Backup

4. To remove a folder, highlight it by clicking on it, then click on the  button. A confirmation window appears (see Figure 5-54).

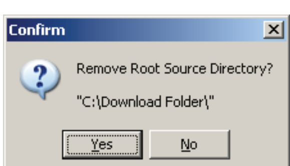
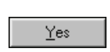


Figure 5-54: Remove Folder Confirmation

5. To remove the folder from the back up directory, click on the  button. The folder is removed from the backup directory (see Figure 5-51 on page 49 of this section).

4.2.1.2 Setup Filters

Filters may be used to exclude or include specific file types in the backup process. The Setup Filters window allows configuration of these filters

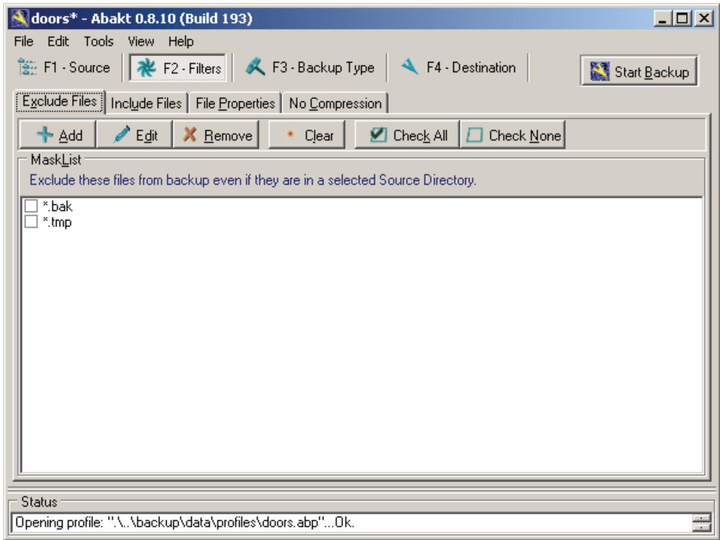


Figure 5-55: Abakt Filters Window

4.2.1.3 Setup Backup Type

Backup Type allows the operator to determine the type of backup to be performed. There are four types of backup to choose from:

- Create New - never overwrite existing backup with the same file name (default value)
- Replace Existing - replace existing backup with the same filename
- Update Existing - add new files and update existing files already present in exiting backup with the same file name
- Freshen Existing - update files already present, don't add new files to existing backup with the same file name

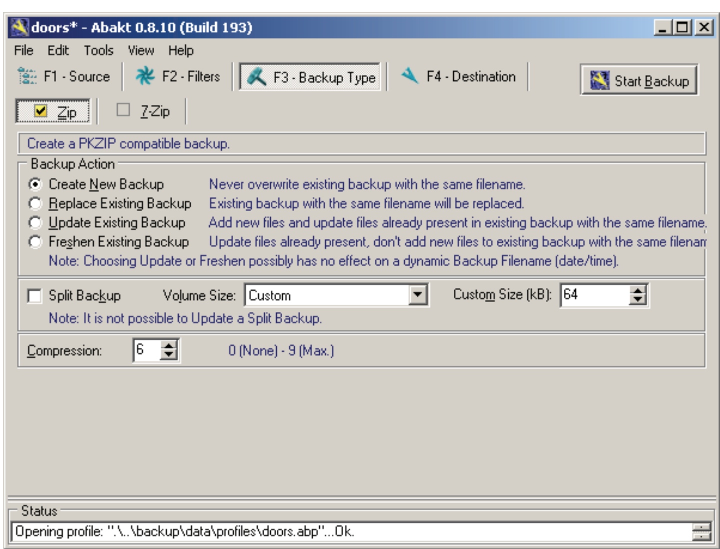


Figure 5-56: Abakt Backup Type Window

4.2.1.4 Setup Destination

The Destination Window allows the operator to select the location for the backed up zip files. The default is set for C:\kerisys\backup\archives.

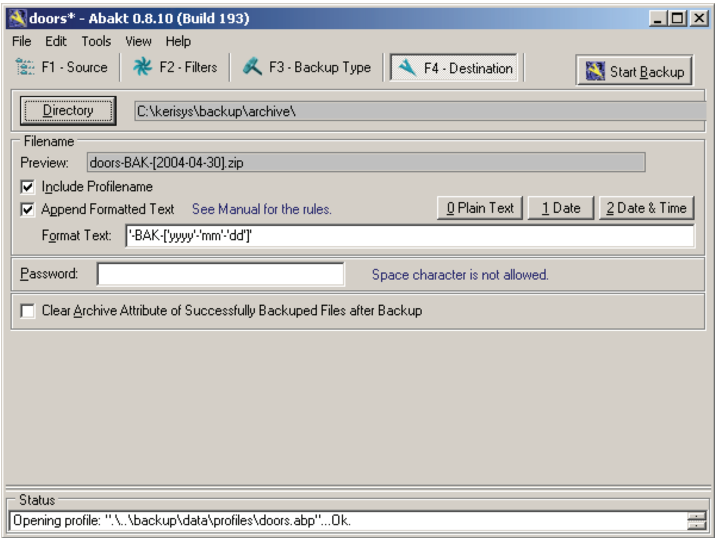
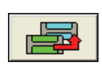


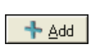
Figure 5-57: Abakt Destination Window

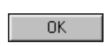
NOTE: The Doors program is automatically closed when Abakt is started. Doors needs to be manually started following any time Abakt has been opened.

4.2.2 Adjusting the Backup Directory

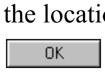
The door.abp file used by the backup program uses the default directory path of C:\Kerisys\DoorsX.XX\ for F1 Source and C:\Kerisys\backup\Archive for F4 Destination. F1 Source is where the files to be backed up are located and F4 Destination is where to place the files selected for back up by F1. This works as it is supposed to, unless the location of the *Doors* installation is changed. The door.abp file is not changed or updated during the install process to reflect where *Doors* is installed. If *Doors* is installed somewhere other than the default locations used in the install program, the following steps must be taken:

1. Open the backup program, by clicking on the  button.
2. Select the “F1 - Source” tab. Click on the 

button. This will remove the default directory path.
3. Click on the 

button. Browse through the folders to find the location of the current *Doors* installation. Select the folder and click on the 

button. The directory path location of the *Doors* installation should now appear in the Directories window in the “F1 - Source” tab.
4. Select the “F4 - Destination” tab. Click on the 

button. Browse through the folders to find the location of the “Kerisys\backup\Archive folder” installation. Select the folder and click on the 

button.
5. Save the changes by clicking on File > Save Profile

NOTE: Steps 1 and 2 need to be done for when an upgrade to a newer version of Doors has been installed.

4.2.3 Perform Backup

1. From the Abakt window (see Figure 5-50 on page 49 of this section), click on the 

button to begin the backup process. All selected files will be backed up into a single compressed ZIP file and saved to the destination directory.

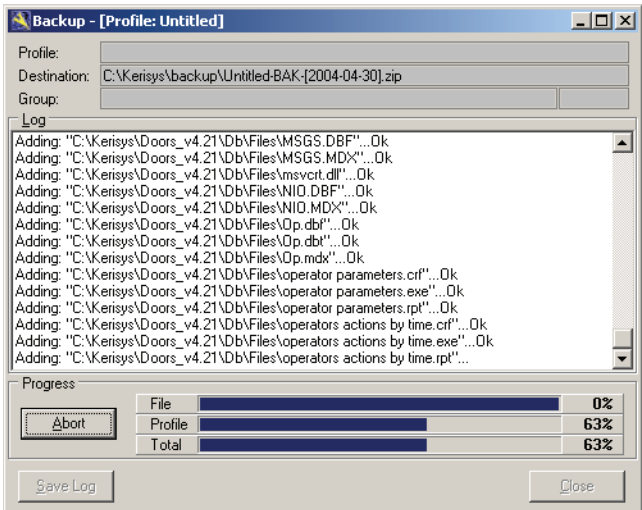


Figure 5-58: Backup in Process

2. Abakt states when the backup process has completed (see Figure 5-59).

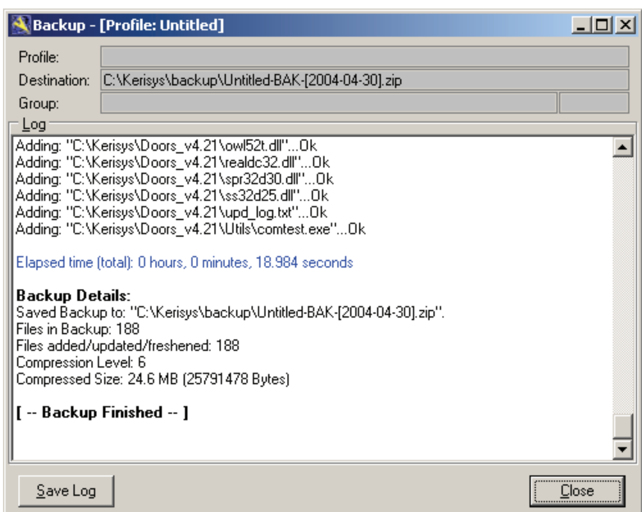


Figure 5-59: Completed Backup Process

3. To close Abakt without saving a copy of the backup log, click on the 

button.
4. To save a copy of the backup log, click on the 

button. A Save Log File window appears (see Figure 5-60 on page 54 of this section).

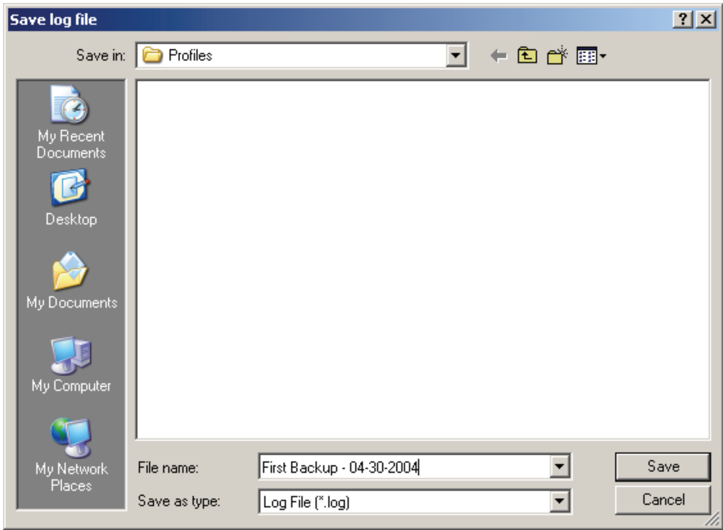


Figure 5-60: Save Backup Log File As

5. Select the location for the log file by using the "Save in" drop down menu.
6. Enter a name for the log file in the "File Name" field.
7. Verify the "Save as Type" field is set to Log File and click on the Save button. The log file is saved to the desired location.
8. Close the Abakt program by clicking on the ☒.

NOTE: The Doors program is automatically closed when Abakt is started. Doors needs to be manually started following any time Abakt has been opened.

NOTE: Backups should be performed on a regular basis. One of the most reliable ways to perform a backup is to set up a Task Scheduler found in Windows 2000 and Windows XP operating systems. Refer to their instructions on how to do this.

4.2.3.1 Archiving the Backup File

It is strongly recommended that the backup ZIP files be archived to another computer or removable media such as CD-R/RW, DVD-R/RW, or tape. Moving the archived files to another computer or removable media gives additional protection of the data.

4.2.4 Restore Backup

Using the built-in backup tool, Abakt, backed up files are contained within an "industry standard" compressed ZIP file. Any ZIP utility (WinZIP, PKZip, for example) may be used to extract the stored information. Abakt may also be used to unZIP the backed up files. The following instructions are for using Abakt to restore backed up files.

<u>Computer Hardware Failure</u>

In the case of a computer hardware failure, the backed up data must have been archived to another computer or removable media (such as CD-R/RW, DVD-R/RW, or tape). Once the computer problem is resolved, use the *Doors* CD-ROM to re-install *Doors* and the Abakt program. Follow the instructions given below to restore the ZIP file.

<u>Database Corruption and Database Rollback</u>

To resolve a database corruption issue or to rollback the database, it is recommended that ALL files be restored. Most *Doors* database files are dependent on other database files. Attempting to restore one database file without restoring all others could result in additional database errors. It is important that the folder that contains the current version of *Doors* be re-named prior to restoring an archived database. Use Windows Explorer to rename the current version of *Doors*. To change the name, locate the folder (default is in C:\kerisys), right click on the *Doors* folder and select Rename. Enter the new name in the field and hit Enter on the keyboard. Follow the instructions given below to restore the ZIP file.

NOTE: When restoring backed up files due to a corrupted database, it is possible that the backed up files also contain the corruption. This could happen if the database files were backed up before the corruption was detected or if Doors was running at the time the backup was performed. In this case, an older version of the backed up database should be selected.

To restore a backed up ZIP file in Abakt.

1. Open Abakt by selecting "Launch Backup" from the *Doors* drop-down menu or click on the  button.
2. To begin the restore backup process, click the Tools ⇒ Restore Backup pull-down menu. The Restore Backup window appears (see Figure 5-61).

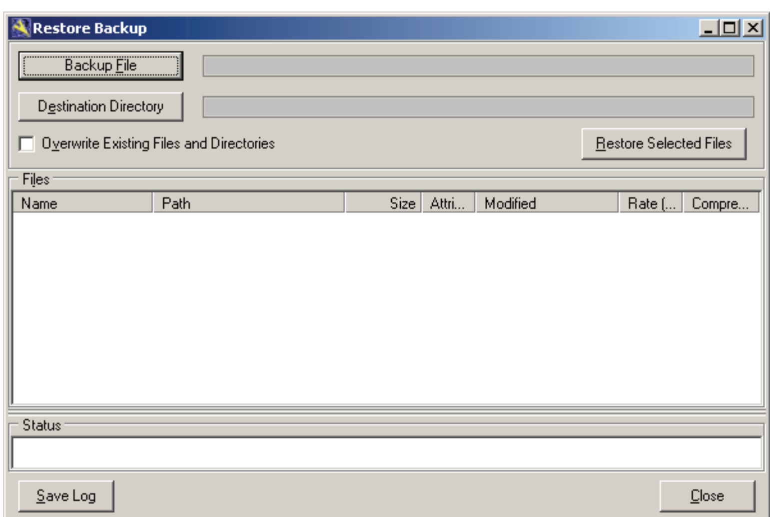


Figure 5-61: Restore Backup Window

3. Click on the 

button. The Select a Backup File to Restore window appears. Select the "archive" folder then the ZIP file to be restored (see Figure 5-62).

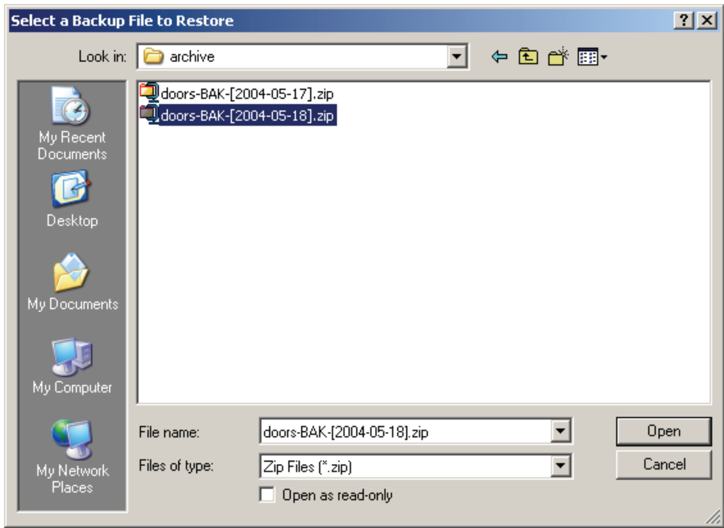


Figure 5-62: Select Backup File to Restore

4. Click on the 

button. The Restore Backup window returns with the backup files entered (see Figure 5-63).

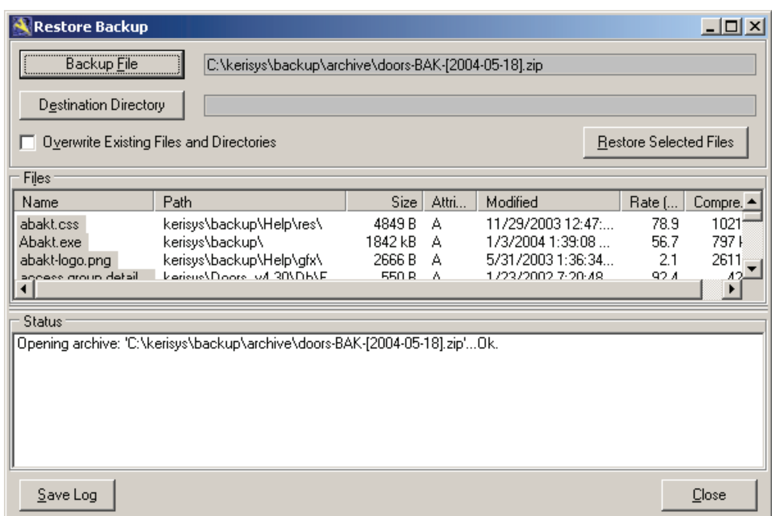


Figure 5-63: Restore Backup Window with Backup Files Entered

5. Click on the Destination Directory button. A browser window appears. Select the folder where the backup will be restored (see Figure 5-64).

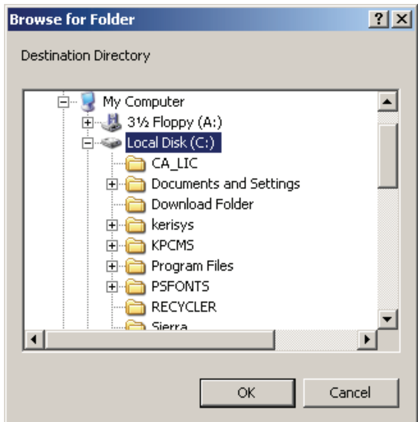


Figure 5-64: Restore Backup Destination

NOTE: The backup ZIP file contains the full path of each file backed up. If Doors was installed in the C:\kerisys folder, selecting the destination of C:\kerisys will cause the backup to be restored to C:\kerisys\kerisys. It is recommended to use the root drive of the hard disk that Doors will be restored to as the destination directory. For example, selecting the destination directory of C: would place the restored files in C:\kerisys\.

6. Once the destination folder has been selected, click on the OK button.

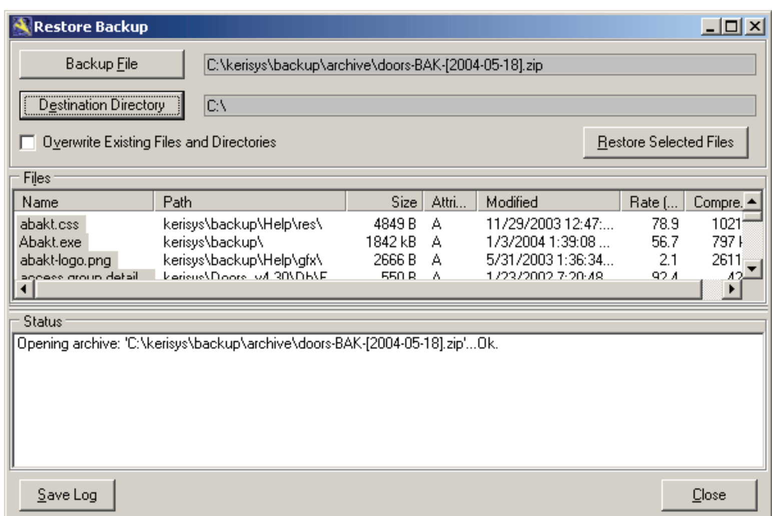


Figure 5-65: Restore Backup Window with Destination Entered

7. Click on the Restore Selected Files button.The files are restored to the C:\kerisys\ folder.

8. To close Abakt without saving a copy of the restore log, click on the Close button.

9. To save a copy of the restore log, click on the Save Log button and follow the steps as outlined previously.

This page is intentionally left blank.

Section 6

System Operation

The system operation section explains how operators can manually and immediately perform the following tasks.

- lock and unlock doors
- suspend and restore auto unlock/lock time zones assigned to doors
- grant anti passback amnesty to users
- set input/output links and perform manual control of i/o

Document Number 01914-006, Revision 5.2 – May, 2004

1.0 Lock, Unlock, Suspend and Restore Doors

The lock and unlock door commands allow an operator to manually override programmed door controls. For lock and unlock commands to remain in effect for extended periods of time, the Auto Unlock/Lock (AUL) time zone must be Suspended; otherwise the lock and unlock command state will return to its AUL state when the AUL time zone boundary is reached, and will continue to operate per the AUL settings. If the AUL is Suspended, the door will follow the operator's manual commands until the operator Restores the door. This can be for hours, days, weeks, indefinitely. To Suspend or Restore the AUL time zone, see “Suspend” on page 14 of this section and “Restore” on page 18 of this section.

The quickest way to determine which doors are in the Suspended state, see “Get Controller Status” on page 39 in section 2.

NOTE: The AUL time zone takes precedence over manual Lock and Unlock commands.

NOTE: The AUL time zone is overridden by Global Unlock, Global Lock, and Continuous Request to Exit (CRTE).

NON Suspended AUL time zones cause the Lock and Unlock commands to operate as follows:

1. If an operator does NOT Suspend the AUL time zone and manually locks a door, that door will remain locked until the AUL time zone dictates the door should be unlocked.
2. If an operator does NOT Suspend the AUL time zone and manually unlocks a door, that door will remain unlocked subject to the type of unlock command. An Unlock command will keep the door unlocked until the AUL time zone dictates the door should be locked. A Timed Unlock command will keep the door unlocked until the door unlock time expires, then the door is locked.

Suspended AUL time zones cause Lock and Unlock commands to operate as follows:

1. If an operator Suspends the AUL time zone and manually locks a door, that door will remain locked until either the operator manually unlocks the door or the operator Restores the AUL time zone and the AUL time zone dictates the door should be unlocked.
2. If an operator Suspends the AUL time zone and manually unlocks a door, that door will remain unlocked until either the operator manually locks the door or the operator Restores the AUL time zone and the AUL time zone dictates the door should be locked.

NOTE: Although specific examples are not provided, these door commands also apply to gates, elevator doors, time and attendance clocks, and EntraGuard doors.

1. To enter the operate door commands window, click on the Operate ⇒ Doors pull-down menu option, or click on the  icon on the tool bar. The Operate Doors window appears (see Figure 6-1 on page 4 of this section).

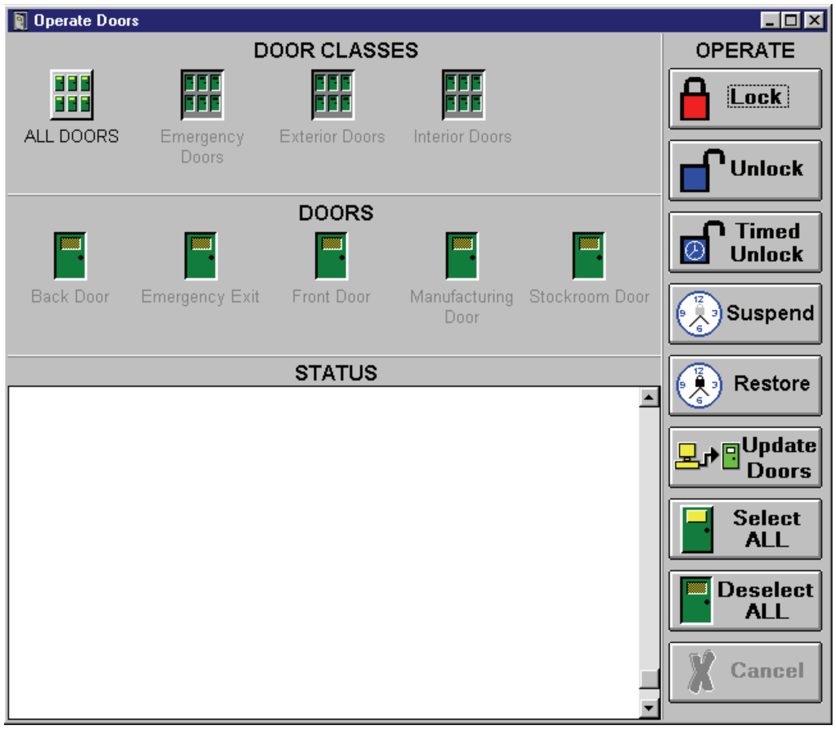


Figure 6-1: Operate Doors Window

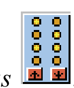
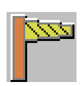
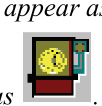
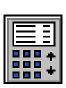
When working with the operate door commands, the following buttons and fields apply to all commands (see Figure 6-1 on page 4 of this section).

- The 

 button selects all doors associated with the selected door class, allowing door operations to be performed on these doors.
- The 

 button deselects all doors associated with the selected door class, not allowing door operations to be performed on these doors.
- The 

 button cancels any operation being performed.
- The **STATUS** field lists each operation that has been performed and the status of that operation.

NOTE: If a door has been designated as an elevator door, its icon will appear as *. If a door has been designated as a gate, its icon will appear as* *. If a door has been designated as a time and attendance clock, its icon will appear as* *. The icon for an EntraGuard controller appears as* .

1.1 Lock Doors

The lock doors command can lock all doors in the access control system, all doors within a door class, or a single door. To lock doors, first select the doors to be locked and then perform the lock command.

1.1.1 Lock All Doors

To lock all doors:

1. Click on the **ALL DOORS** icon under Door Classes.
2. Click on the 

button, and then click on the 

button. The resulting window should look similar to Figure 6-2.

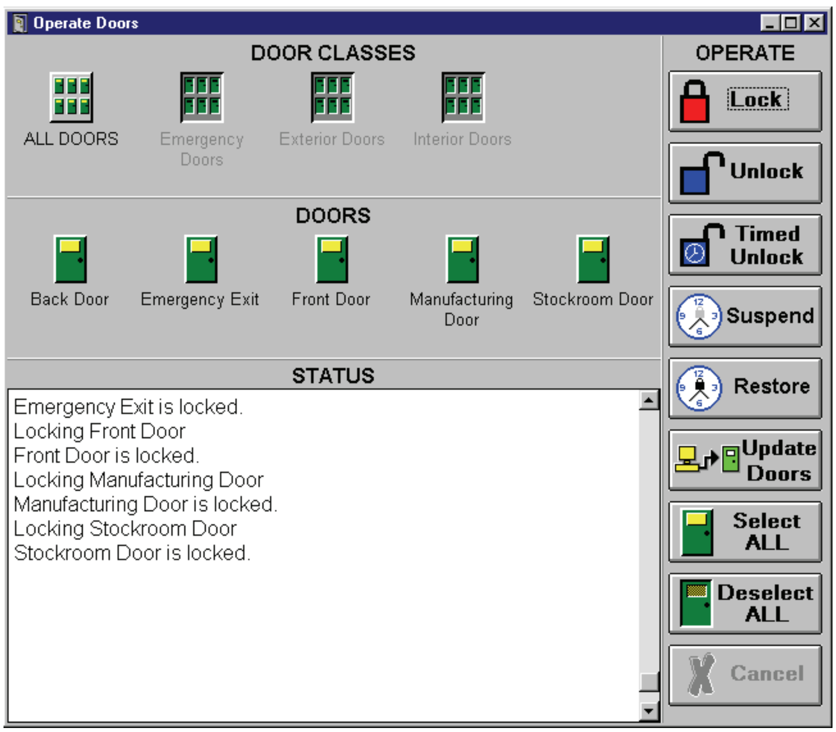


Figure 6-2: Locking All Doors

1.1.2 Lock All Doors in a Door Class

To lock all doors in a door class; for example, the Exterior Doors door class (refer to “Assign a Door Class” on page 28 in section 3 for information regarding door classes):

1. Click on the icon for the door class to be locked; under Door Classes, click on the **Exterior Doors** icon.
2. Click on the 

button, and then click on the 

button. In this example, the Exterior Doors door class was selected; the resulting window will look similar to Figure 6-3.

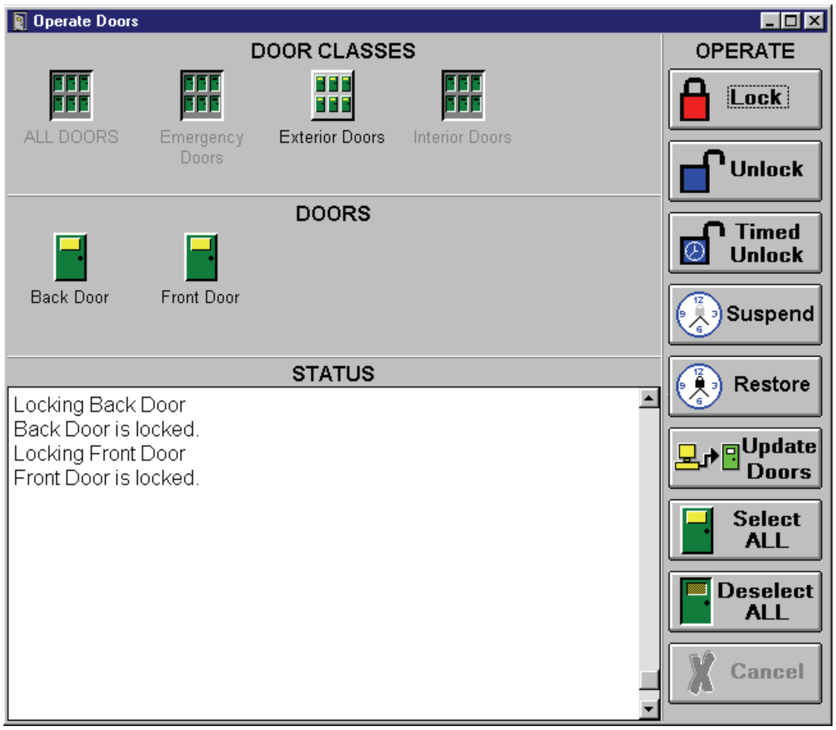


Figure 6-3: Locking All Doors in a Door Class

1.1.3 Lock a Single Door

To lock a single door; for example, the Stockroom Door:

1. Locate the door to be locked. Either click on the **All Doors** icon or click on the door group icon the door is listed under. For this example, click on the **Interior Doors** door group icon.
2. Locate and click on the icon for the door to be locked. For this example, click on the **Stockroom Door** icon.
3. Click on the 

button. The resulting window will look like Figure 6-4.

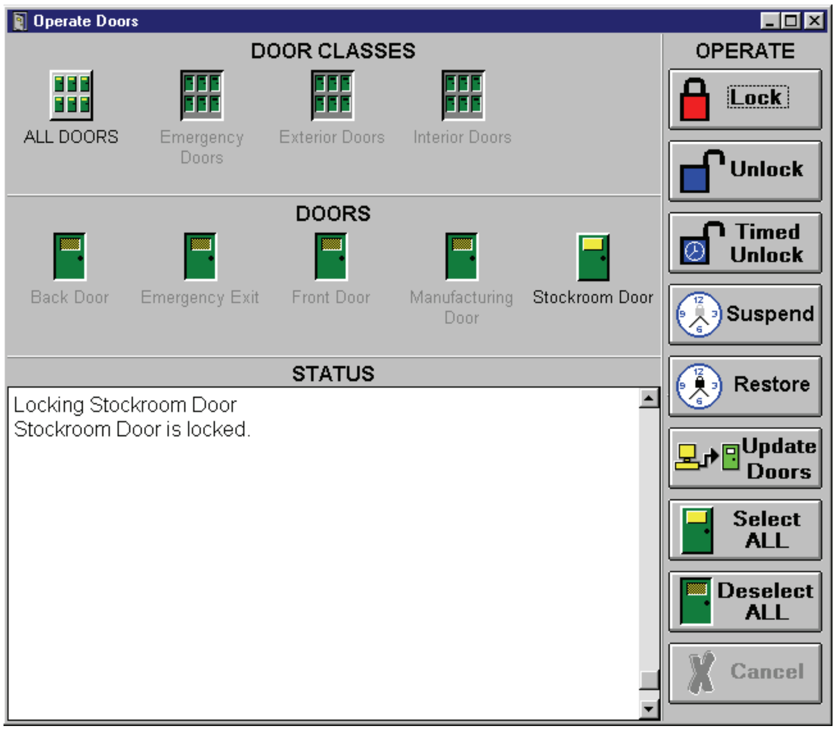


Figure 6-4: Locking a Single Door

1.2 Unlock Doors

The unlock doors command can unlock all doors in the access control system, all doors within a door class, or a single door. To unlock doors, first select the doors to be unlocked and then perform the unlock command.

1.2.1 Unlock All Doors

To unlock all doors:

1. Click on the **ALL DOORS** icon under Door Classes.
2. Click on the 

button, and then click on the 

button. The resulting window should look similar to Figure 6-5.

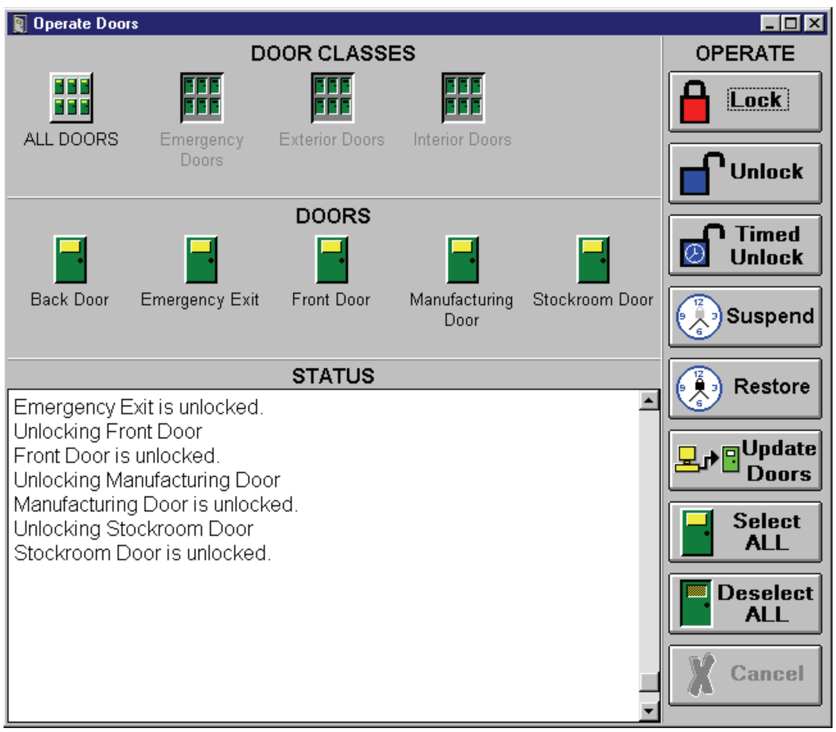


Figure 6-5: Unlocking All Doors

1.2.2 Unlock All Doors in a Door Class

To unlock all doors in a door class (refer to “Assign a Door Class” on page 28 in section 3 for information regarding door classes):

1. In the Door Classes field, click on the icon for the door class to be unlocked.
2. Click on the 

button, and then click on the 

button. The resulting window will look similar to Figure 6-6.

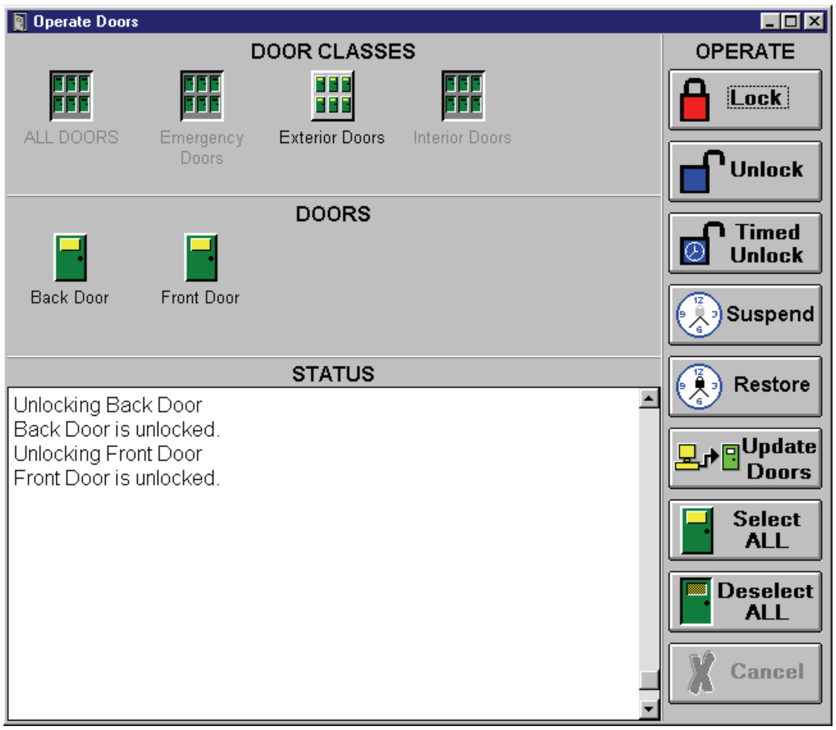


Figure 6-6: Unlocking All Doors in a Door Class

1.2.3 Unlock a Single Door

To unlock a single door:

1. Locate the door to be unlocked. In the Door Classes field, click on either the **All Doors** icon or the Door Class icon of the door to be unlocked.
2. Locate and click on the icon for the door to be unlocked.
3. Click on the 

button. The resulting window will look similar to Figure 6-7.

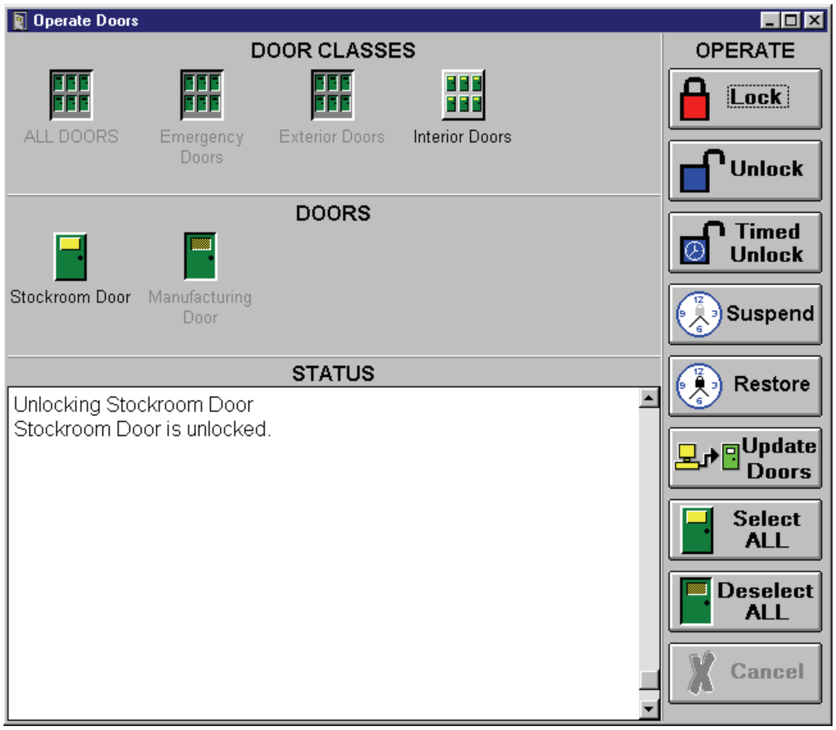


Figure 6-7: Unlocking a Single Door

1.3 Timed Unlock

The timed unlock doors command unlocks a door until the door's unlock time expires or until the door is closed; then it re-locks the door. This command can timed unlock all doors in the access control system, all doors within a door class, or a single door. To timed unlock doors, first select the doors to be unlocked and then perform the timed unlock command (refer to "Set a Door Unlock Time" on page 32 in section 3 for information regarding door unlock times).

1.3.1 Timed Unlock All Doors

To perform a timed unlock on all doors:

1. Click on the **ALL DOORS** icon under Door Classes.
2. Click on the 

button, and then click on the 

button. The resulting window should look similar to Figure 6-8.

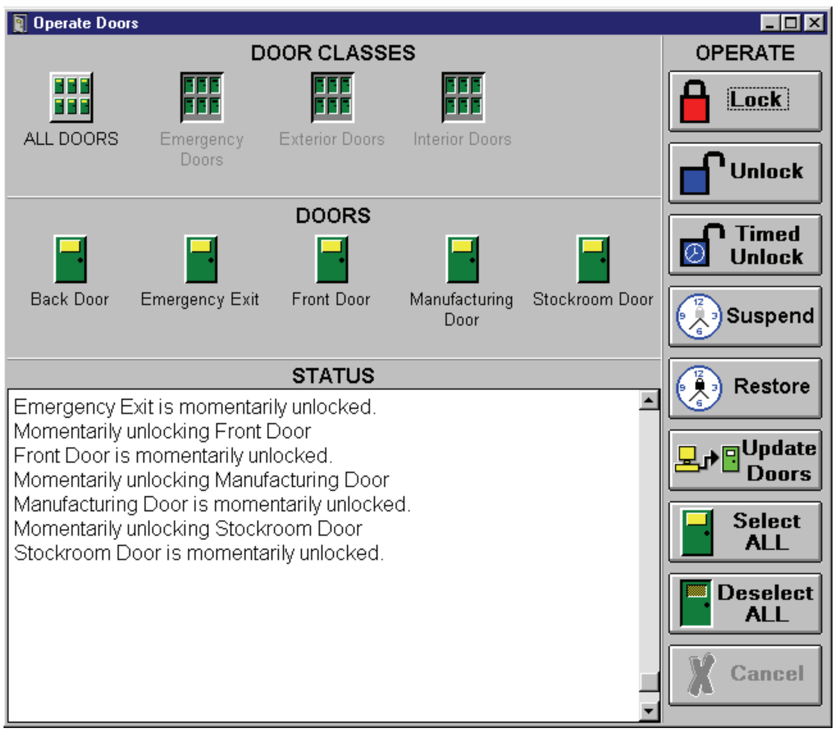


Figure 6-8: Timed Unlocking All Doors

1.3.2 Timed Unlock All Doors in a Door Class

To perform a timed unlock on all doors in a door class (refer to “Assign a Door Class” on page 28 in section 3 for information regarding door classes):

1. In the Door Classes field, click on the icon for the door class to be timed unlocked.
2. Click on the 

button, and then click on the 

button. The resulting window will look similar to Figure 6-9.

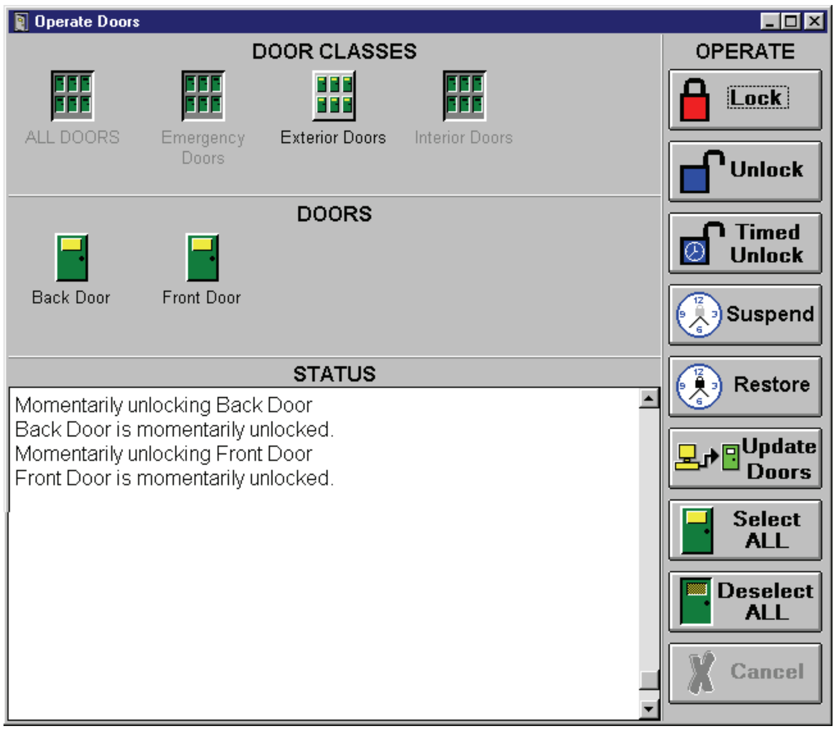


Figure 6-9: Timed Unlocking All Doors in a Door Class

1.3.3 Timed Unlock a Single Door

To performed a timed unlock on a single door:

1. Locate the door to be timed unlocked. Either click on the **All Doors** icon or click on the door class icon the door is listed under.
2. Locate and click on the icon for the door to be timed unlocked.
3. Click on the  button. The resulting window will look similar to Figure 6-10.

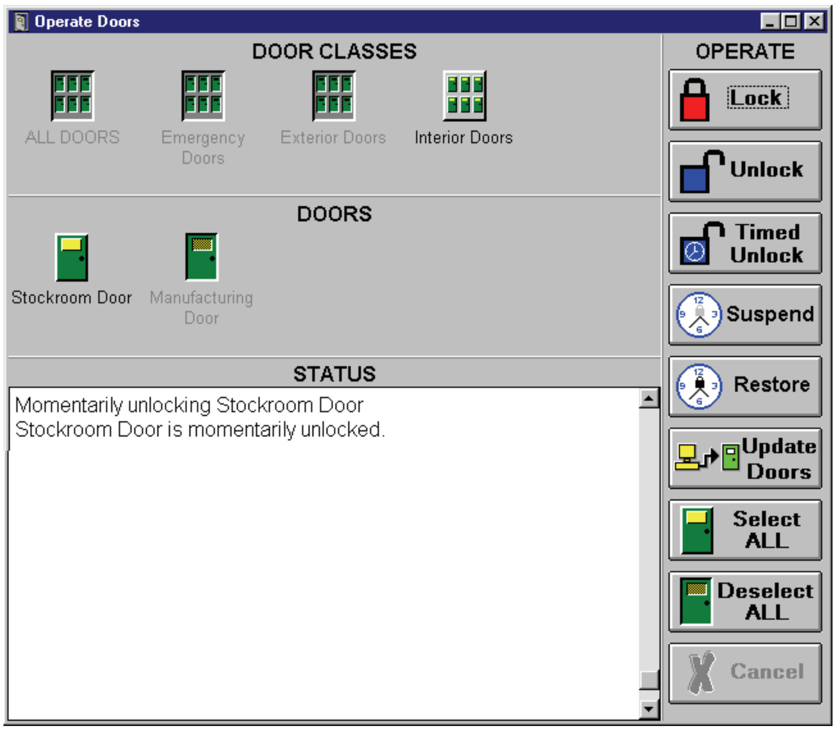


Figure 6-10: Timed Unlocking a Single Door

1.4 Suspend/Restore Auto Unlock/Lock

Auto Unlock/Lock (AUL) time zones allow an operator to configure Doors to be automatically locked and unlocked per the hours defined in a time zone. This feature is applied to doors individually in the Setup ⇒ System ⇒ Doors menu. A pull-down list allows the operator to select the applicable time zone. If a door's AUL time zone is set to Never that door will not automatically unlock/lock.

For temporary, manual control, the Operate ⇒ Doors window provides commands that allow you to override the current AUL time zone setting for individual doors.

1.4.1 Suspend

The Suspend feature allows an operator to Suspend any AUL time zone applied to a particular door or set of doors.

Suspend affects AUL time zones in these ways.

1. When an operator Suspends a door's AUL time zone function, the door is prevented from following its assigned AUL time zone.
2. If a door is within its AUL time zone (the door is unlocked) and you Suspend AUL, the door is locked and will not follow the AUL time zone until manually Restored.
3. If a door is outside of its AUL time zone (the door is locked) and you Suspend AUL, the door remains locked and will not follow the AUL time zone until manually Restored.

1.4.1.1 Suspend Auto Unlock/Lock on All Doors

To Suspend auto unlock/lock time zones on all doors:

1. Click on the **ALL DOORS** icon under Door Classes.
2. Click on the 

button, and then click on the 

button. A window appears reminding the operator that doors with a Suspended Auto Unlock/Lock time zone must be manually Restored (see Figure 6-11).

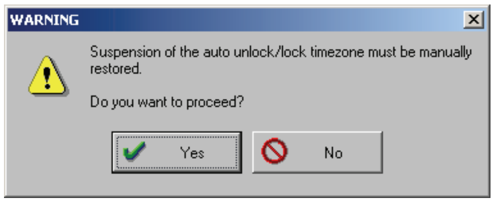
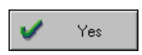


Figure 6-11: Suspend Auto Unlock/Lock Reminder

3. To cancel the Suspend AUL, click on the 

button.
4. To proceed with the Suspension, click on the 

button. The resulting window should look similar to Figure 6-12.

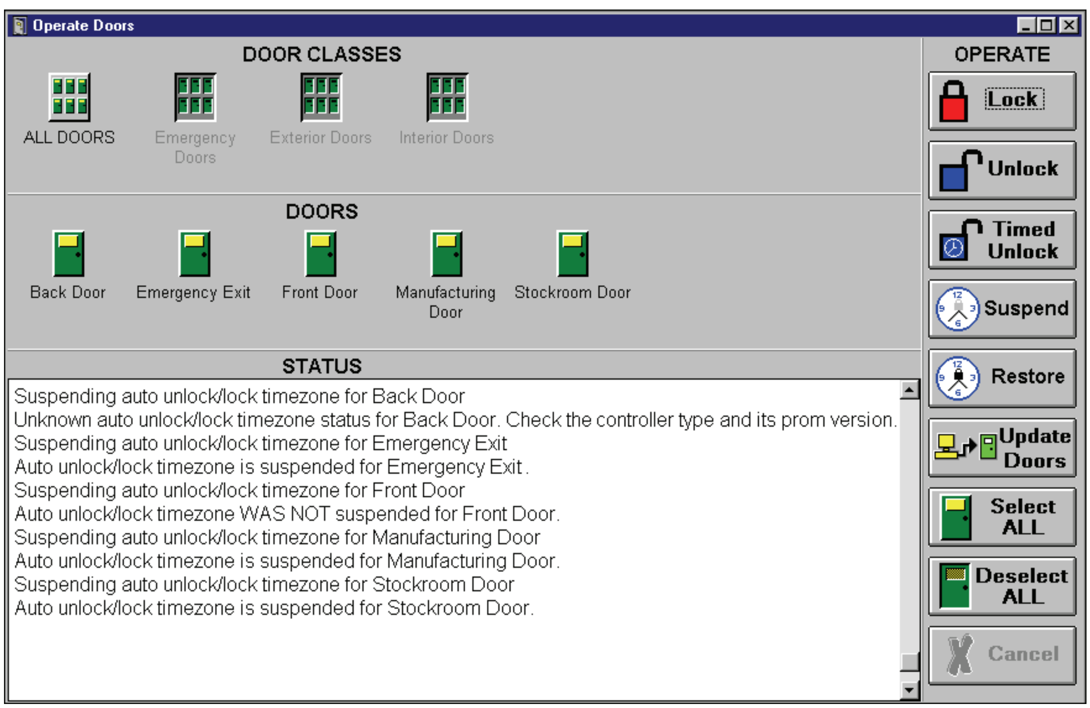


Figure 6-12: Suspending Auto Unlock/Lock on All Doors

1.4.1.2 Suspend Auto Unlock/Lock on All Doors in a Door Class

To Suspend auto unlock/lock on all doors in a door class (refer to “Assign a Door Class” on page 28 in section 3 for information regarding door classes):

1. In the Door Classes field, click on the icon for the door class to be Suspended.
2. Click on the 

button, and then click on the 

button. A window appears reminding the operator that doors with a Suspended Auto Unlock/Lock must be manually Restored (see Figure 6-13).

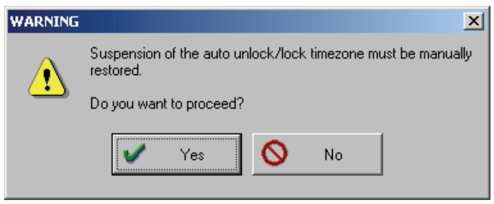
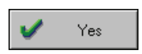


Figure 6-13: Suspend Auto Unlock/Lock Reminder

3. To cancel the Suspend AUL, click on the 

button.
4. To proceed with the Suspension, click on the 

button. The resulting window should look similar to Figure 6-14.

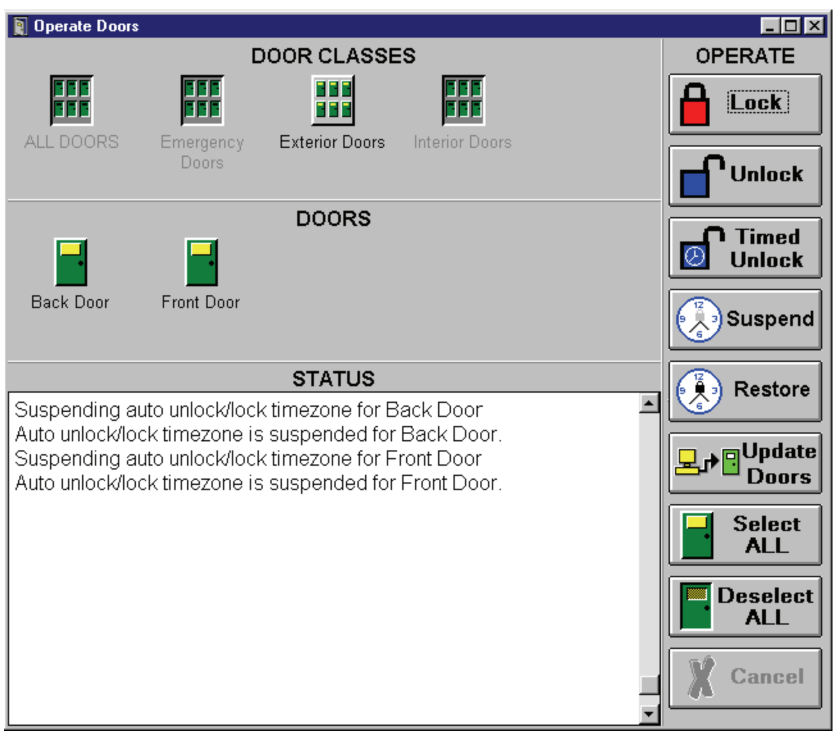


Figure 6-14: Suspending Auto Unlock/Lock on All Doors in a Door Class

1.4.1.3 Suspend Auto Unlock/Lock on a Single Door

To Suspend auto unlock/lock on a single door:

1. Locate the door to be Suspended. Either click on the **All Doors** icon or click on the door class icon the door is listed under.
2. Locate and click on the icon for the door to be Suspended.
3. Click on the 

button. A window appears reminding the operator that doors with a Suspended Auto Unlock/Lock must be manually Restored (see Figure 6-15).

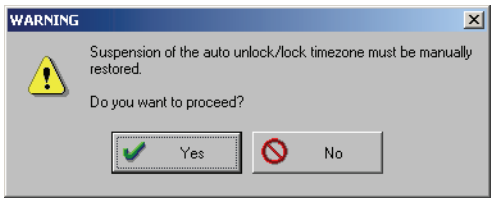
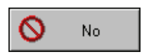
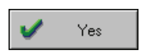


Figure 6-15: Suspend Auto Unlock/Lock Reminder

4. To cancel the Suspend AUL, click on the 

button.
5. To proceed with the Suspension, click on the 

button. The resulting window should look similar to Figure 6-16.

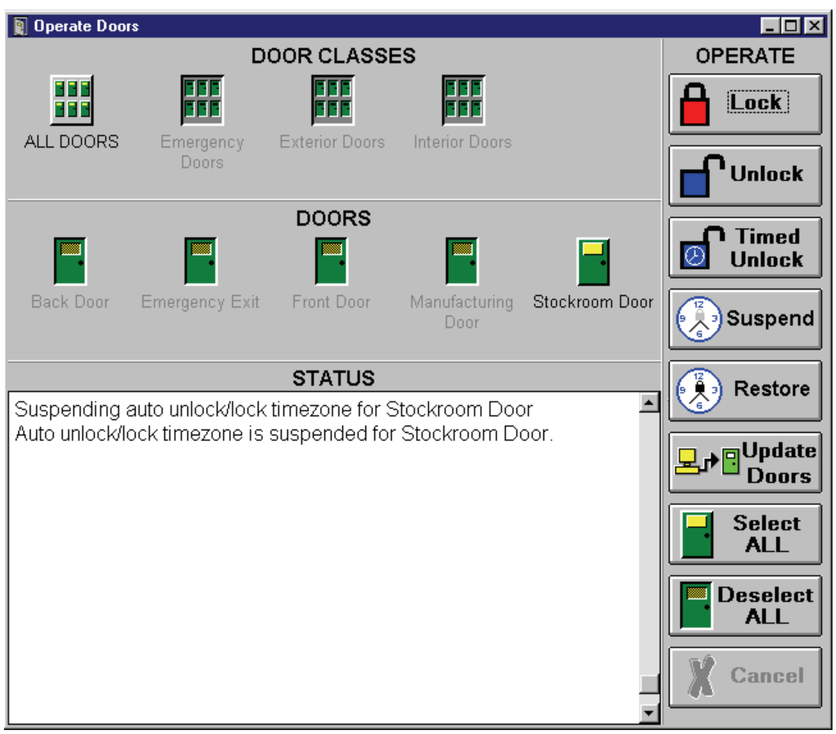


Figure 6-16: Suspending Auto Unlock/Lock on a Single Door

1.4.2 Restore

The Restore feature allows an operator to Restore any Suspended AUL time zone applied to a particular door or set of doors.

Restore affects AUL time zones in these ways.

1. Restoring a door's AUL time zone allows the door to follow its assigned AUL time zone.
2. If a door is within its AUL time zone (the door should be unlocked) and you Restore AUL, the door remains unlocked and continues to operate per its AUL time zone.
3. If a door is outside of its AUL time zone (the door is locked) and you Restore AUL, the door remains locked, but will unlock per its AUL time zone and continue operating per its AUL time zone.

1.4.2.1 Restore Auto Unlock/Lock on All Doors

To Restore auto unlock/lock on all doors:

1. Click on the **ALL DOORS** icon under Door Classes.
2. Click on the 

button, and then click on the 

button. A confirmation window appears (see Figure 6-17).

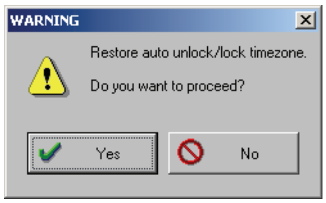
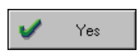


Figure 6-17: Restore Auto Unlock/Lock Confirmation

3. To cancel the Restore AUL, click on the 

button.
4. To proceed with the Restore, click on the 

button. The resulting window should look similar to Figure 6-18.

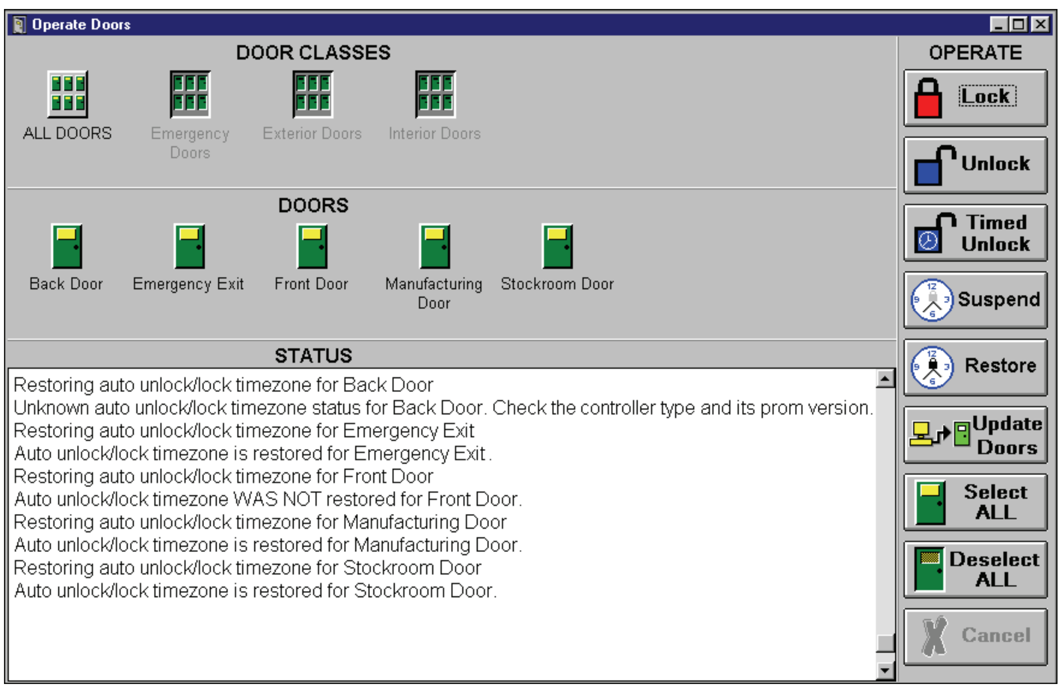


Figure 6-18: Restore Auto Unlock/Lock on All Doors

1.4.2.2 Restore Auto Unlock/Lock on All Doors in a Door Class

To Restore auto unlock/lock on all doors in a door class (refer to “Assign a Door Class” on page 28 in section 3 for information regarding door classes):

1. In the Door Classes field, click on the icon for the door class to be Restored.
2. Click on the 

button, and then click on the 

button. A confirmation window appears (see Figure 6-19).

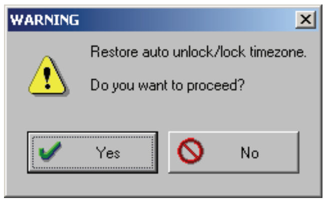
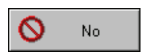
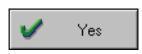


Figure 6-19: Restore Auto Unlock/Lock Confirmation

3. To cancel the Restore AUL, click on the 

button.
4. To proceed with the Restore, click on the 

button. The resulting window should look similar to Figure 6-20.

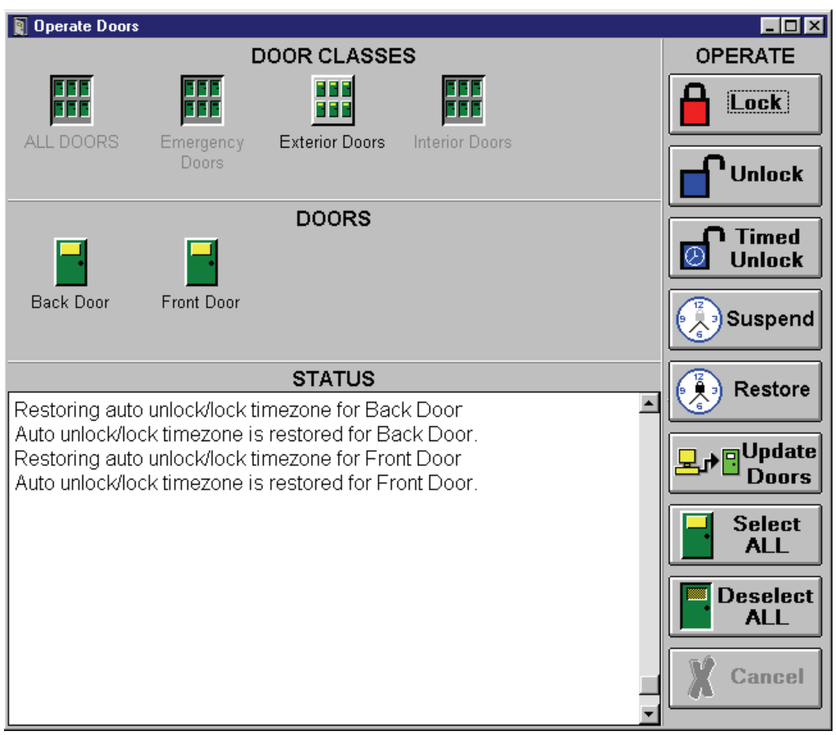


Figure 6-20: Restore Auto Unlock/Lock on All Doors in a Door Class

1.4.2.3 Restore Auto Unlock/Lock on a Single Door

To Restore auto unlock/lock on a single door:

1. Locate the door to be Restored. Either click on the **All Doors** icon or click on the door class icon the door is listed under.
2. Locate and click on the icon for the door to be Restored.
3. Click on the  button. A confirmation window appears (see Figure 6-21).

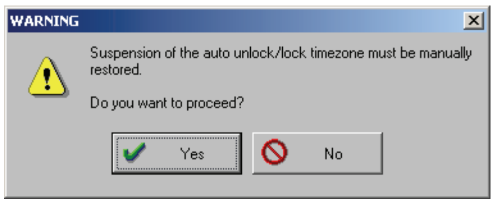
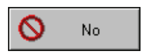
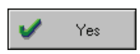


Figure 6-21: Restore Auto Unlock/Lock Confirmation

4. To cancel the Restore AUL, click on the  button.
5. To proceed with the Restore, click on the  button. The resulting window should look similar to Figure 6-22.

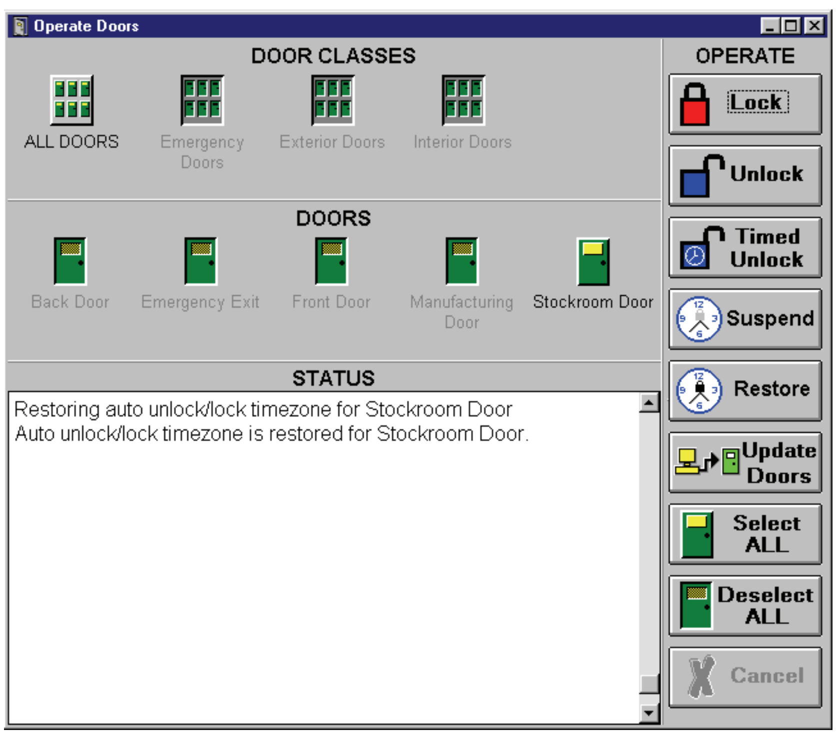


Figure 6-22: Restore Auto Unlock/Lock on a Single Door

2.0 Update Doors

Updating doors completely rewrites all database information stored on the selected controllers (as opposed to the update net command which only updates changes in databases). This command can update all doors in the access control system, all doors within a door class, or a single door. To update doors, first select the doors to be updated and then perform the update command.

As an update doors command is a complete rewrite of ALL databases on the designated controllers, it takes longer to perform than an update net command. When an update doors command is performed, please be patient as data is transferred. Depending upon the number of controllers and the size of the databases, this operation can take an extended period of time to perform.

NOTE: Updating doors resets the APB amnesty value for all cardholders (see "Set Local Anti Passback" on page 13 in section 2).

2.1 Update All Doors

To update all doors:

1. Click on the **ALL DOORS** icon under Door Classes.

2. Click on the 

button, and then click on the 

button. A series of status windows appear (see Figure 6-23), tracking the data being transferred to all the doors/controllers.

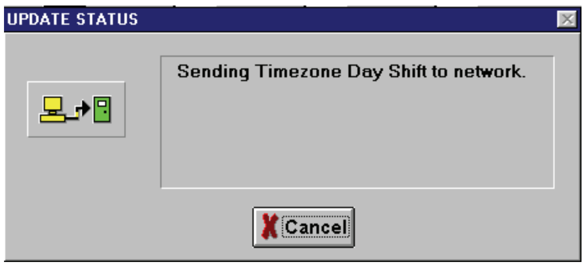


Figure 6-23: Transferring Data Status Windows

3. Once the complete data transfer process is complete, the resulting window should look similar to Figure 6-24.

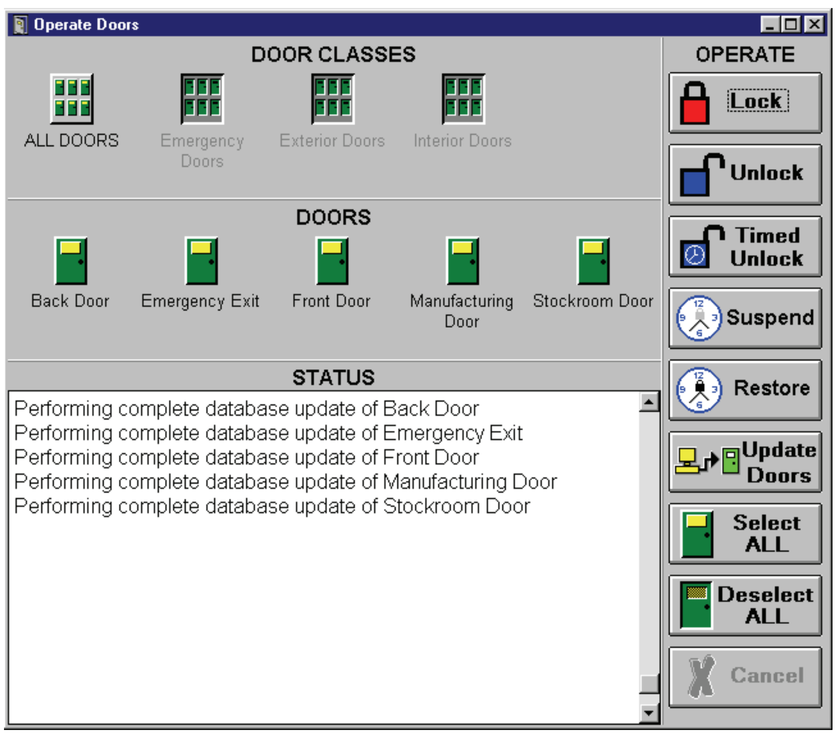


Figure 6-24: Update All Doors

2.2 Update All Doors in a Door Class

To update all doors in a door class (refer to “Assign a Door Class” on page 28 in section 3 for information regarding door classes):

1. In the Door Classes field, click on the icon for the door class to be updated.
2. Click on the 

button, and then click on the 

button. A series of status windows appear (see Figure 6-23 on page 23 of this section), tracking the data being transferred to all the doors/controllers. The resulting window will look similar to Figure 6-25.

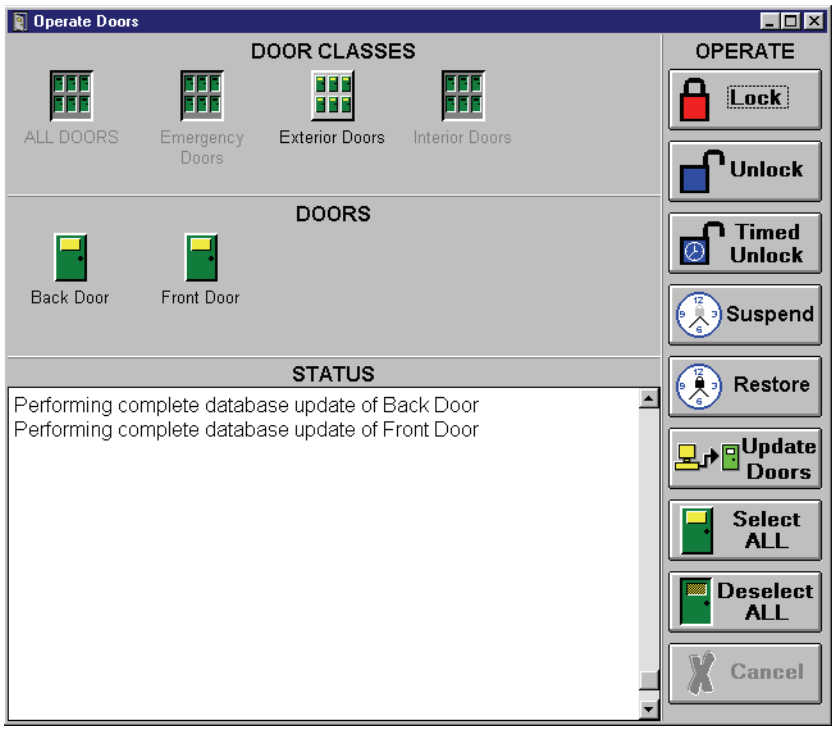


Figure 6-25: Updating All Doors in a Door Class

2.3 Update a Single Door

To update a single door:

1. Locate the door to be updated. Either click on the **All Doors** icon or click on the door class icon the door is listed under.
2. Locate and click on the icon for the door to be updated.
3. Click on the 

button. A series of status windows will appear (see Figure 6-23 on page 23 of this section), tracking the data being transferred to all the doors/controllers. The resulting window will look similar to Figure 6-26.

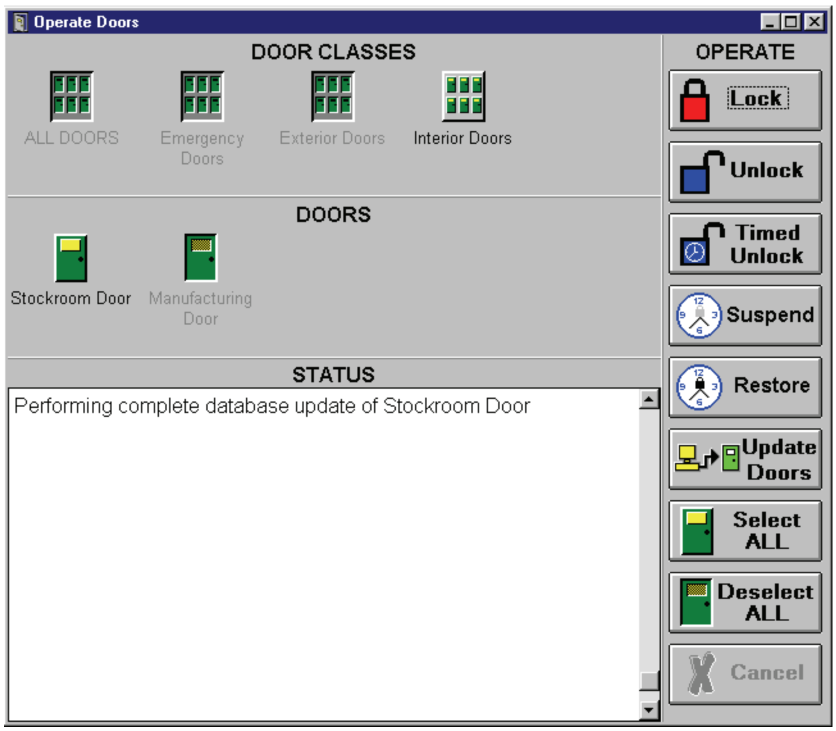


Figure 6-26: Updating a Single Door

3.0 Anti Passback Amnesty

The grant anti passback amnesty (APB) command allows an operator to immediately grant anti passback amnesty to an individual user, to selected users, or to all users in the access control network.

1. To enter the grant APB amnesty window, click on the Operate ⇒ Amnesty pull-down menu option. The Grant Amnesty window appears (see Figure 6-27). This window includes a list of all users eligible to be granted APB amnesty.

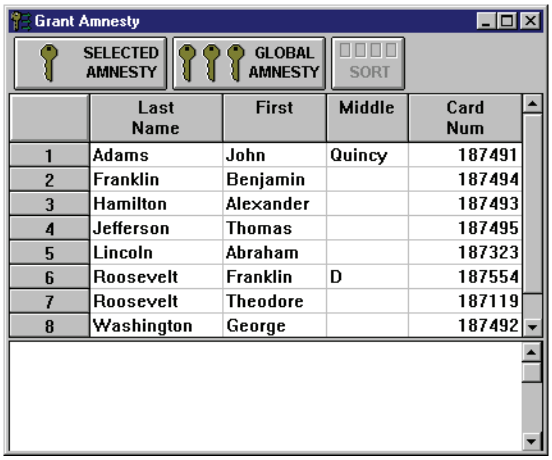


Figure 6-27: Grant Anti Passback Amnesty Window

NOTE: If the word Amnesty is missing from the pull-down menu, you have not enabled Local APB during the system setup. See "Set Local Anti Passback" on page 13 in section 2 for instructions on how to change your selection. If the word Amnesty is greyed out in the pull-down menu, the operator does not have permission to grant amnesty (see "Setup Operators" on page 45 in section 2).

3.1 Granting Amnesty to a Selected User

To grant APB amnesty to a selected user:

1. Scroll through the list of users eligible to be granted APB amnesty and locate the desired user.
2. Click on that user's name. The name becomes highlighted indicating it has been selected (see Figure 6-28).

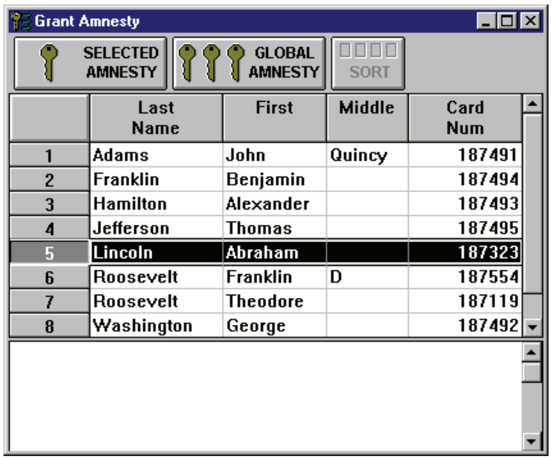


Figure 6-28: Selected Single User to Grant APB Amnesty

3. Click on the  button at the top of the window.

4. The result of the operation is then displayed in a results field at the bottom of the Grant Amnesty window (see Figure 6-29).

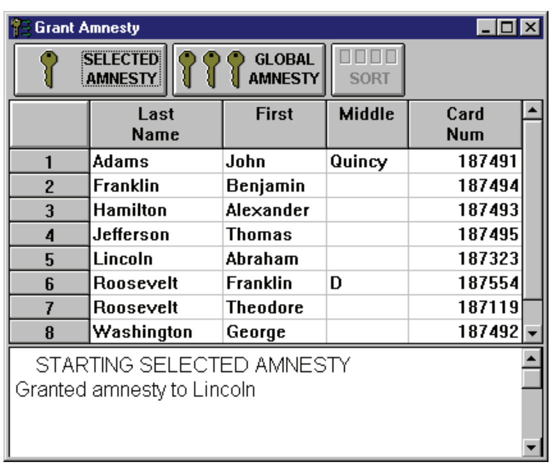


Figure 6-29: Results of Selected User Granted APB Amnesty

3.2 Granting Amnesty to Selected Users

To grant APB amnesty to selected users:

1. Users can be selected in two ways.

- Hold down the “Ctrl” key. Scroll through the list of users eligible to be granted APB amnesty and locate the desired users. As a user is located, click on that user’s name. The name becomes highlighted indicating it has been selected. See Figure 6-30.

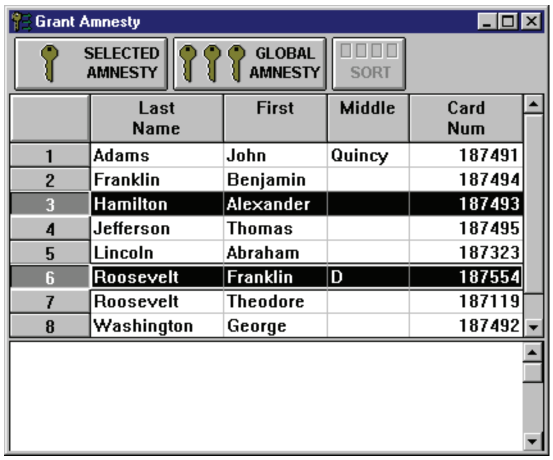


Figure 6-30: Selected Multiple Users to Grant APB Amnesty

- If the desired users are in sequential order, click on the user’s name at the top of the list, hold down the “Shift” key, and click on the user’s name at the end of the list. All names from top to bottom become highlighted indicating they all have been selected. See Figure 6-31.

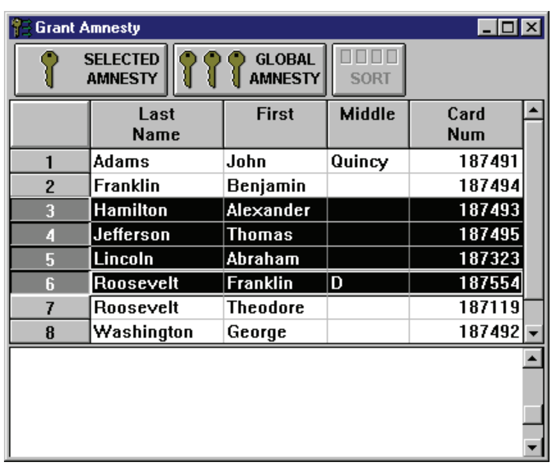


Figure 6-31: Sequentially Selected Multiple Users to Grant APB Amnesty

2. Click on the 

button at the top of the window.
3. The result of the operation is then displayed in a results field at the bottom of the Grant Amnesty window (see Figure 6-32 on page 29 of this section).

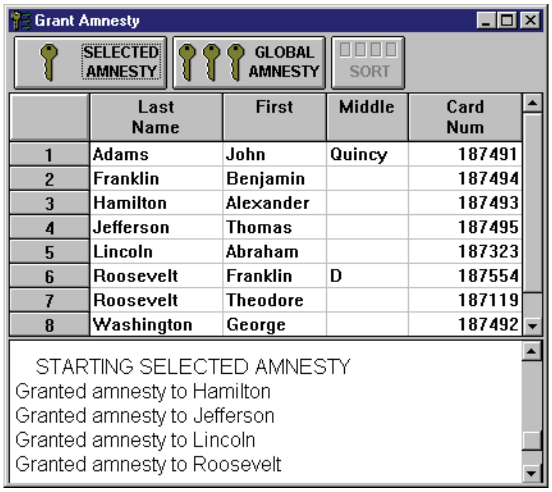


Figure 6-32: Results of Selected Multiple Users Granted APB Amnesty

3.3 Granting Global Amnesty

The Global Amnesty command grants amnesty to all users in the access control network.

1. To grant global amnesty simply click on the 

button at the top of the window.
2. The result of the operation is then displayed in a results field at the bottom of the Grant Amnesty window (see Figure 6-33).

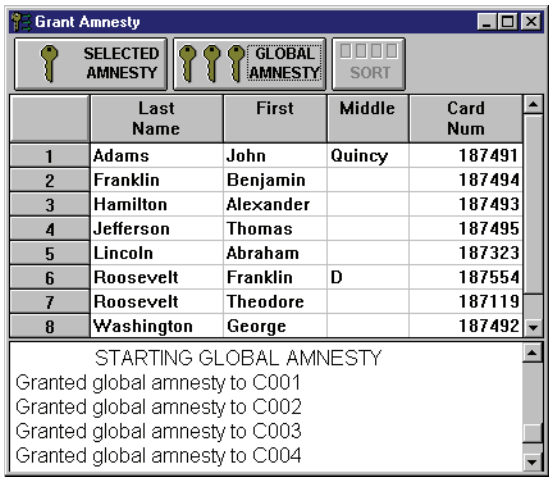


Figure 6-33: Results of Grant Global APB Amnesty

NOTE: Granting global amnesty causes an event to be recorded for every card/cardholder that can be granted APB amnesty. If there is a large number of cardholders, there is a potential for the controller event buffers to fill with amnesty granted messages, causing the oldest existing events on the controller to be overwritten. This is because once the buffer fills, the newest events received overwrite the oldest events in the buffer and events are written to the buffer faster than they can be downloaded from the controllers. The Controller Reports Events command can be used to filter out the granting of global amnesty messages (see "Controller Reports Events" on page 21 in section 5), but the ability to track the granting of global amnesty is then lost.

3.4 Sorting Users

The sort data button allows an operator to display the users in the spreadsheet in a desired order (always from A to Z or from lowest to highest number). Users can be sorted by any of the user name fields or by the card number. Sorting allows an operator to group user data in a manner that makes it easy to locate those users to which amnesty should be granted. In this example, a sort by card number will be performed.

1. Click on the Card Num column header. The entire column is highlighted (see Figure 6-34).

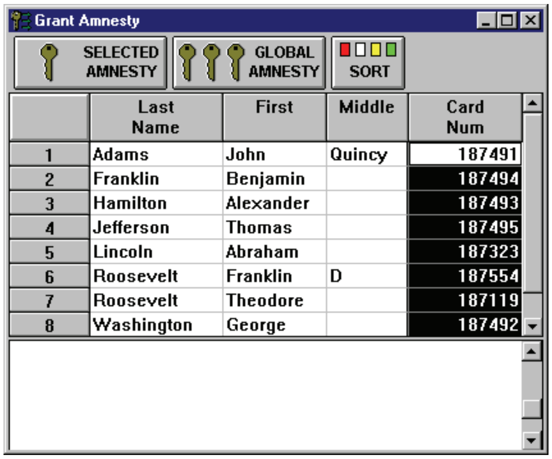


Figure 6-34: Preparing to Sort User Data by Card Number

2. Click on the  button. All data in the spreadsheet is now reorganized by card number from the lowest number to the highest number. (see Figure 6-35).

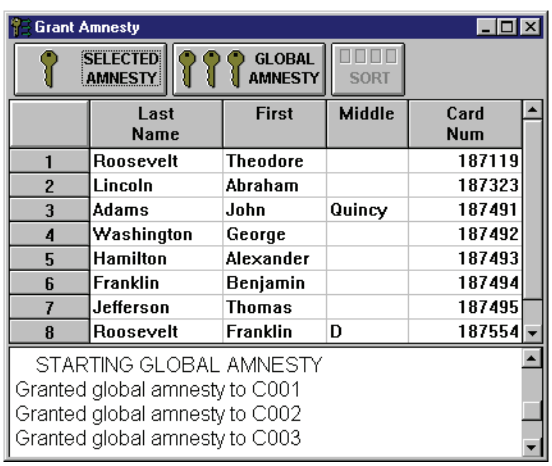


Figure 6-35: User Data Sorted by Card Number

4.0 I/O Control

The I/O control feature allows an operator to have input events drive output responses. For example, an input connected to a vibration sensor or glass-break detector on a window can be linked to an alarm output so that a broken window will sound an alarm.

I/O control is managed through the I/O Config and Link Config tabs in the Setup System window. I/O Configuration defines the input and output points, and Link Configuration ties the inputs to the outputs.

Certain I/O points are dedicated to specific input/output functions (i.e. the RTE input, the door switch input, the door lock output, the door alarm output). These points are not available for I/O control assignment (refer to "Configure Dedicated I/O Points" on page 17 in section 3).

Manual control for output points is also available, allowing an operator to manually turn-on/enable or turn-off/disable an output point. This allows an operator to control an output point and to override a link event that is driving an output.

4.1 I/O Configuration

The I/O Config tab displays the input and output points that are available per controller (see Figure 6-36 on page 33 of this section). An operator can assign a descriptive name to every non-dedicated input and output point and can identify if an input is normally-open or normally-closed. Grey input and output point name fields indicate those inputs and outputs are dedicated by the controller and are not available for link assignment.

The following steps describe how to configure an input point and an output point for window monitoring as described above. For this example, controller 3 is a PXL-250 controller with an SB-293 Satellite board. This satellite board is configured for 2-door control. Using dedicated I/O, one input is automatically configured for auxiliary RTE and one output is automatically configured for door held open alarm annunciation. This leaves 5 inputs and 1 output that can be programmed into I/O links.

1. To configure input/output points, click on the Setup ⇒ System pull-down menu or click on the  button on the tool bar. Then click on the **I/O Config** tab.
2. Click on the  arrow in the "Controller" field and a list of the controllers with available I/O points appears. Scroll through this list and click on the controller which has the I/O points to be configured. For this example, you would click on controller **C003**.
3. Locate an available input point for assignment. For example, locate input point 4.
4. To assign a name to the input point, click in the Input Point Name field for the desired input point and type the name to be assigned to the point. For example, for Input Point Name 4, type **Window Sensors**.
5. The normal state for this input is normally-closed. If a window is broken the input will be opened. For the Mode of Input Point 4, click on the **N/C** radio button.
6. To assign a name to an output point, double click in the Output Point Name field for the desired output point and type the name to be assigned to the point. For Output Point Name 4, type **Window Alarm**.
7. The resulting window should appear similar to Figure 6-36 on page 33 of this section.

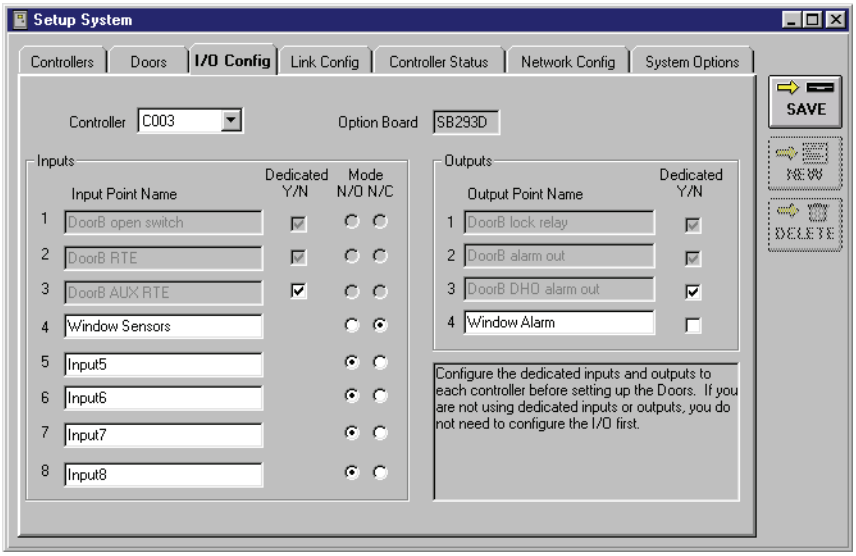


Figure 6-36: Input/Output Point Definitions

8. Click on the 

button. If the new I/O configuration information is not saved before clicking any other button or exiting the Setup System window the data entered is lost and must be re-entered.

9. Now update the access control network with the new information. Click on the 

button on the tool bar (for details on the update process refer to “Update the Network” on page 35 in section 5).

4.2 Link Configuration

The Link Config tab allows an operator to customize the controller's output responses to events at the controller's inputs (see Figure 6-37). Input points can be linked to output points, allowing a change of state at an input to activate an output relay. Blank input and output point name fields indicate those inputs and outputs are reserved by the controller for door control and are not available for link assignment. The following rules apply for link configuration.

- Up to 32 links can be defined per controller.
- Any input can be used by all 32 links.
- Inputs on a controller can only be linked to outputs on the same controller.
- Multiple inputs can be linked to multiple outputs using OR/AND functions allowing an operator to create complex input/output links.
- Outputs on one controller can be hard-wired to inputs on other controllers.

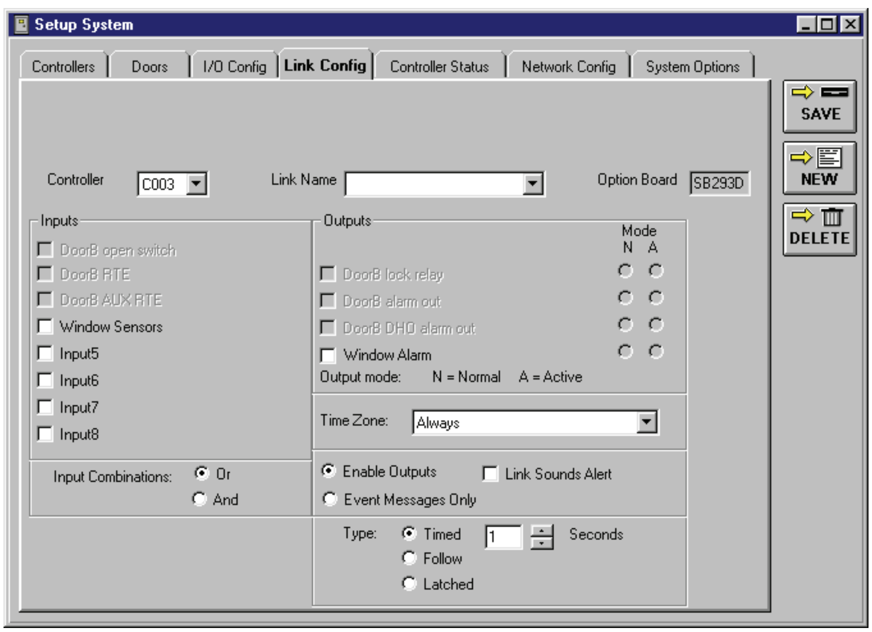


Figure 6-37: Link Configuration Window

4.2.1 Link Parameters

The following list is the parameters that need to be configured when defining an I/O link. Refer to Figure 6-37 to locate the parameter fields. Following this list is an example of an I/O Link.

Controller

The Controller field allows the operator to select the controller with I/O links to be configured.

1. Click on the  arrow in the "Controller" field and a list of the controllers with available I/O points appears.
2. Scroll through this list and click on the controller which has the I/O points to be configured.

Link Name

To assign a descriptive name to a link:

1. Click in the “Link Name” field.
2. Type the name to be assigned to the link.

Option Board

The “Option Board” field displays the model number of the option board providing the input and output points. This is an information field and is not editable.

Inputs

The “Inputs” check boxes allow an operator to select the inputs that should be assigned to the I/O link. Inputs with grayed-out check boxes and without input point names are unavailable for assignment.

1. Click on the check box beside the input point name. A check mark appears indicating the input is selected. Every click in the check box toggles between selecting and deselecting.
2. To deselect an input, click on the check box. The check mark disappears indicating the input is deselected.

Input Point Name

The “Input Point Name” field displays the input point name assigned in the I/O Configuration section. In this window, this field is not editable. To change an input point name, refer to “I/O Configuration” on page 32 of this section.

Input Combinations

The “Input Combinations” radio buttons allow an operator to define what the state of the selected inputs should be to generate an output. This is only valid if there are more than one input point being applied to the I/O link.

1. If the Or radio button is selected, an input signal on the first input point or the second input point or any of the input points will generate an output. Click on the **Or** radio button to select an Or input combination.
2. If the And radio button is selected, an input signal must be received on the first input point and the second input point and all of the input points at the same time to generate an output. Click on the **And** radio button to select an And input combination.

Outputs

The “Outputs” check boxes allow an operator to select the outputs that should be assigned to the I/O link. Outputs with grayed-out check boxes and no output point name are not available for assignment.

1. Click on the check box beside the output point name. A check mark appears indicating the output is selected. Every click in the check box toggles between selecting and deselecting.
2. To deselect an output, click on the check box. The check mark disappears indicating the output is deselected.

Output Point Name

The Output Point Name field displays the output point name assigned in the I/O Configuration section. In this window, this field is not editable. To change an output point name, refer to “I/O Configuration” on page 32 of this section.

Output Mode

The “Output Mode” radio buttons allow an operator to define if the output relay should be driven to its active state or its normal state when an output is generated.

1. Driving to the active state opens the normally closed contact and closes the normally open contact. Typically, this is used to turn on an alarm or device. Click on the **A** radio button to select the active state.
2. Driving to the normal state closes the normally closed contact and opens the normally open contact (the normal or idle state of the relay). Driving an output to the normal state can be used to turn off an output that was driven to its active mode. Click on the **N** radio button to select the normal state.

Enable Outputs

The “Enable Outputs” and “Event Messages Only” radio buttons work in conjunction with each other. One or the other can be selected, not both.

1. Click on the Enable Outputs radio button to select if the input events in the I/O link should drive an output relay.
2. Click on the Event Messages Only radio button to select if the input events in the I/O link should just generate an event message.

Event Messages Only

See Enable Outputs.

Link Sounds Alert

Links a sound alert to the I/O link that will annunciate when in monitor mode.

Output Alarm Type

The “Output Alarm Type” radio buttons allow an operator to select how long an output is driven when activated. There are three output modes from which to choose.

- Click on the **Timed** radio button to make the output relay active for the period of time defined in the Seconds field. To set a time in the Seconds field, either double-click in the field and directly type in a value (255 seconds maximum) or use the  arrows to scroll up and down and select a time.
- Click on the **Follow** radio button to make the output relay follow the state of the input. The output will stay active as long as the input is in its active state. When the input becomes inactive, the output becomes inactive. A Follow output uses two links internally which reduces the total number of available links.
- Click on the **Latched** radio button to have the output state triggered by the input state. When the input becomes active, the output becomes active and stays active until manually inactivated by an operator (using the manual output control commands given in the next section or by another link).

Time Zone

The “Time Zone” field allows an operator to assign a time zone to the I/O link. The entering or exiting of the time zone time period does not activate the link; the link will operate only during the time period defined by that time zone.

1. Click on the  arrow. A list of all available time zones appears.
2. Scroll through this list and click on the desired time zone. If the link must be active all the time, click on the Always time zone.

4.2.2 I/O Link Example

The following steps describe how to link an input point to an output point for window monitoring using the example described in the I/O configuration section above. For this example, controller 3 is a PXL-250 controller with an SB-293 Satellite board. This satellite board is configured for 2-door control. Using dedicated I/O, one input is automatically configured for auxiliary RTE and one output is automatically configured for door held open alarm annunciation. This leaves 5 inputs and 1 output that can be programmed into I/O links.

1. To configure an input/output link, click on the Setup ⇒ System pull-down menu or click on the  button on the tool bar. Click on the **Link Config** tab.
2. Click on the Controller  arrow and select the controller to be configured.
3. Click in the Link Name field and type in the name for the link. For this example type **Window Security** (see Figure 6-38).

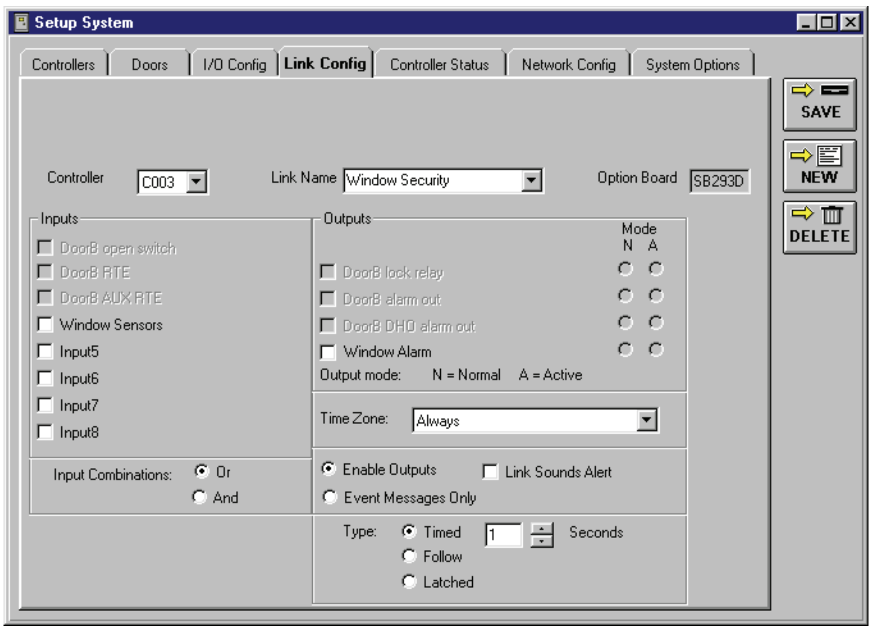


Figure 6-38: Select Controller and Enter I/O Link Name

4. Click on the **Input 4** check box to select the Window Sensors input point (see Figure 6-39 on page 38 of this section). Since this is a single input point, the Input Combination radio buttons do not apply.
5. Click on the **Output 4** check box to select the Window Alarm output point (see Figure 6-39 on page 38 of this section).

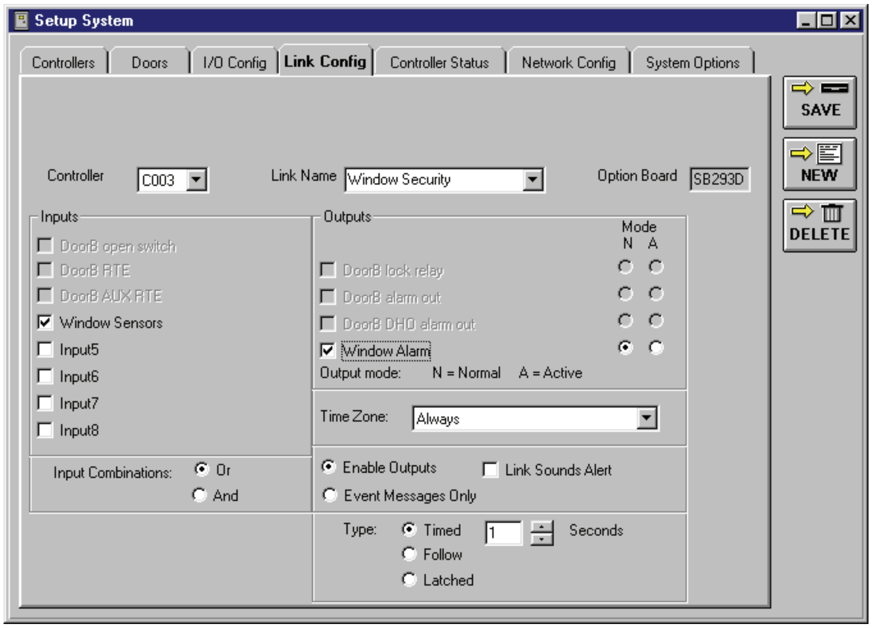


Figure 6-39: Select Input and Output Points

6. Click on the **A**ctive output mode radio button to have the link drive the output relay to its active state, sounding an alarm.
7. Click on the **Enable Outputs** radio button to activate the output relay (this is the default value for outputs).
8. Click on the **Latched** output alarm type to have the alarm stay on until manually turned off.
9. Click on the  arrow and select **Activate Alarms** from the list of available time zones.
10. The completed I/O Link should appear similar to Figure 6-40.

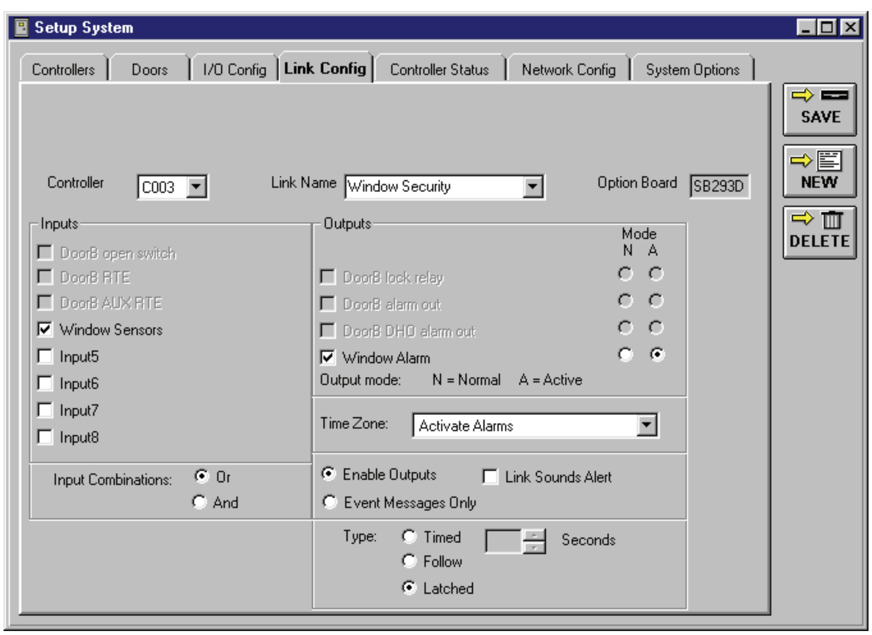


Figure 6-40: The Completed Window Alarms I/O Link

11. Click on the 

button. If the new I/O Link is not saved before clicking any other button or exiting the Setup System window the data entered is lost and must be re-entered.

12. Now update the access control network with the new information. Click on the 

button on the tool bar (for details on the update process refer to "Update the Network" on page 35 in section 5).

4.3 Manual Output Control

Manual control for output points allows an operator to manually turn-on/enable or turn-off/disable an output point. This allows an operator to control an output point and to override a link event that is driving an output.

Following the window alarm example above, an operator can use the manual output control feature to manually test the window alarm periodically.

1. To manually control output points, click on the Operate ⇒ Output Control pull-down menu. A window similar to Figure 6-41 appears.

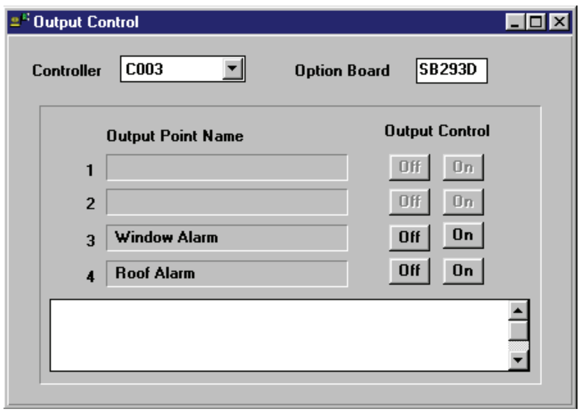


Figure 6-41: Output Control Window

2. Under the Output Point Name list, locate the output point to manually control. For this example, locate output point 3 – the Window Alarm.
3. Under the Output Control Off/On buttons, click on the On button to turn-on/enable an output point.
4. Under the Output Control Off/On buttons, click on the Off button to turn-off/disable an output point.
5. The status field at the bottom of the window displays the results of the operations performed (see Figure 6-42).

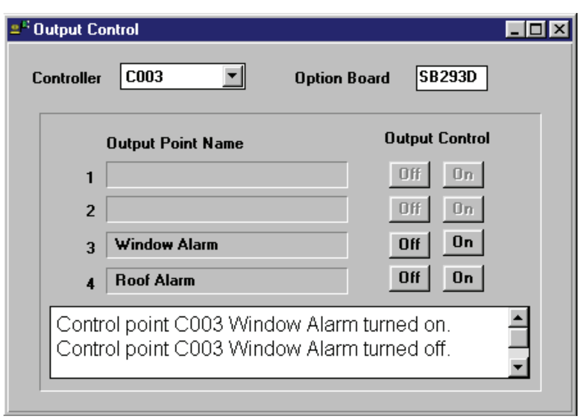


Figure 6-42: Toggled Output Points

Section 7

Reporting

There are three types of event reports: formatted reports, quick search reports, and power search reports. In order to make sure you have the most up to date information, collect all event information from the controllers before generating a report (see “Collecting Events While Updating” on page 38 in section 5 or “Collecting Events While Monitoring” on page 46 in section 5). If you are going to retrieve any information for dates that have been archived, restore those files before attempting to generate a report (see “Restoring Archived Files” on page 29 in section 5).

- In formatted reports, the operator selects from a list of pre-programmed reports.
- In a quick search, the operator selects search parameters from a short list of commonly used search criteria.
- In a power search, the operator creates a search expression from lists of events, boolean operators, event values, and linking operators. Once created, power search expressions can be saved in a library for future use.

Document Number 01914-007, Revision 5.5 – April, 2006

1.0 Formatted Report

Formatted reports have been pre-programmed to make it easier for the operator to view and print basic system and event information. There are two types of formatted reports available.

- event reports – allows the operator to select a specific date range
- system parameters reports – allows the operator to view system configurations

1. To use a formatted report, click on the Reports ⇒ Reports pull-down menu option, or click on the  icon on the tool bar. The Formatted Reports window appears (see Figure 7-1).

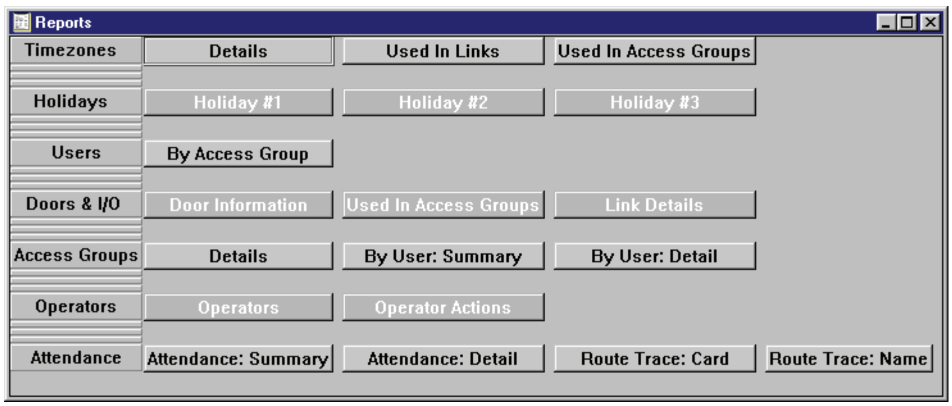


Figure 7-1: Formatted Reports Window

NOTE: The spreadsheet font size chosen in "Set the Spreadsheet Font" on page 44 in section 2 will affect the look of this window. If you have chosen a small font size (anything smaller than 11), some of the report names may be cut off.

2. Click on the name of the report you want to see. For this example, click on the **Time In Building: Summary** report. Since this is an event report, the Event File Date Range window will appear (see Figure 7-2). If you select a system parameters report, skip to step 7.

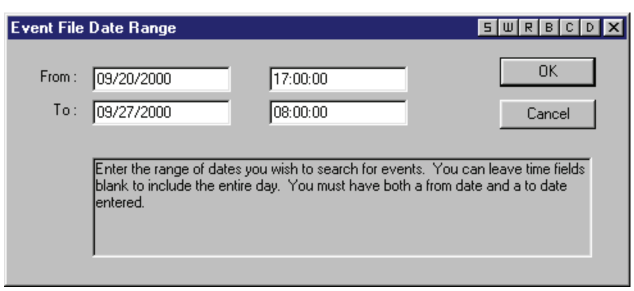


Figure 7-2: Event File Date Range Window

3. To select dates between specific days, click on the **From. . . To** radio button. The default is for the **From. . . To** fields to display today's date.
4. In the From field, enter the beginning date and time for reporting events. If the time field is left at the default of 00:00:00, the events from the beginning of the day (Midnight) are reported. For example, to report on events beginning on September 20, 2000 at 17:00 hours, double-click in the From date field and type **09/20/2000**. Double-click in the From time field and type **17:00:00** (see Figure 7-2).

5. In the To field, enter the ending date and time for reporting events. If the time field is left at the default of 23:59:59, the events from the entire day are reported. For example, to report on events ending on September 27, 2000 at 08:00 hours, double-click in the To date field and type **09/27/2000**. Double-click in the To time field and type **08:00:00** (see Figure 7-2 on page 3 of this section). Click on the 

button.
6. If there is no data that meets the date range you have entered, an empty report warning window appears (see Figure 7-3). Click on the 

button and modify the date selection in the Event File Date Range window (see Figure 7-2 on page 3 of this section).

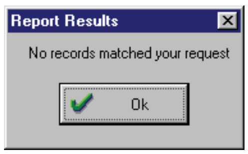


Figure 7-3: Empty Report Warning Window

7. Once you have entered a valid date range, the Report Options window will appear (see Figure 7-4). You are now ready to generate the report output.

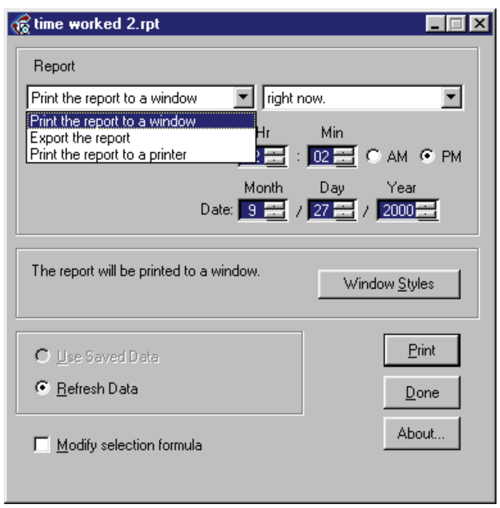


Figure 7-4: Report Options Window

NOTE: Before generating a formatted report, verify the Refresh Data radio button is selected and the Modify selection formula is not selected. Failure to do this may cause incorrect information to be displayed in the report.

1.1 Available Formatted Reports

The following is a list with a short description of the Formatted Reports that are currently available (see Figure 7-1 on page 3 of this section).

Timezones

- Details - Lists the start and stop times of each time zone.
- Used In Links - Lists individual time zones and all associated I/O links (including link name, site, and controller number).
- Used In Access Groups - Lists time zones and all associated access groups and reader names.

Holidays

- Holiday #1 - Lists all dates defined in Holiday #1
- Holiday #2 - Lists all dates defined in Holiday #2
- Holiday #3 - Lists all dates defined in Holiday #3

Users

- By Access Group - Listing of all users, sorted by access group.

Doors & I/O

- Door Information - Listing of door configuration, sorted by site then individual door. Report shows site name, door name, controller number, door number, auto unlock, unlock time, (door) type, open alarm, and first person in.
- Used In Access Groups - Lists all doors with the associated access groups and time zones.
- Link Details - Detailed listing of all I/O links. Report shows link name, input points, type, output points, time zone, link enabled, and output type.

Access Groups

- Details - Listing of all access groups with the associated doors and time zones.
- By User: Summary - Summary listing of access groups and time zones associated with individual users. Report is sorted by user's last name and card/ID number.
- By User: Detail - Detailed listing of access groups and time zones associated with individual users. Report is sorted by user's last name and card/ID number showing specific start and stop times of time zones assigned.

Operators

- Operators - Listing of all operators and their assigned setup/operation parameters.
- Operator Actions - Listing of all operators showing actions taken with date and time log.

Attendance

- Attendance: Summary - Summary of time spent in a building by user. Report is sorted by card number and shows total amount of time spent in the building. The exceptions column notifies you of any time period exceeding 12 hours indicating a possible APB violation.
- Attendance: Detail - Detailed listing of the time spent in building by a user. Listing shows card number, user's name, door name, direction of reader, and time and date of last access. Report is sorted by card number and shows total amount of time spent in building. The exceptions column notifies you of any time period exceeding 12 hours indicating a possible APB violation.
- Route Trace: Card - Traces the movement of a single card through the system by listing the user's name, door accessed, direction of the reader (in, out, or non-directional), and date and time of the access. This report is sorted by date and time.
- Route Trace: Name - Traces the movement of a user through the system by listing the user's name, door accessed, direction of the reader (in, out, or non-directional), and date and time of access. This report is sorted by date and time.

NOTE: If you have more than one user with the same first and last names, information for both users will be combined on the Route Trace: Name report as though they were one person.

1.2 Generate Formatted Report Output

Once a report has been selected, there are three formats for generating the formatted report output.

- view the report on the computer
- save the report to file
- print the report

1.2.1 View Report on Screen

1. To view the formatted report on the computer, click on the on the left side of the “Report” field in the Report Options window and select Print the report to a window (see Figure 7-4 on page 4 of this section).
2. To select when you want to view the report, click on the on the right side of the “Report” field and select “right now” (see Figure 7-4 on page 4 of this section).
3. In the central field, click on the Window Styles button. The Window Style Options window will appear (see Figure 7-5).

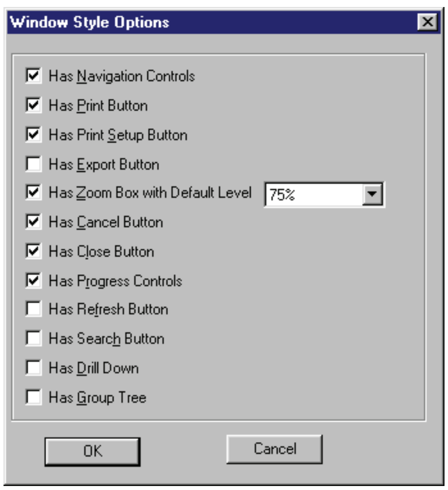


Figure 7-5: Window Style Options

4. Select the options you want to show in your window view by clicking on the box next to the selection and a check mark will appear. To de-select an option, click on the box again and the check mark disappears.

NOTE: Be sure to select the “Print Setup Option.” The orientation of the report can only be changed in the print setup screen accessed through this button.

5. Once all your options have been chosen, click on the OK button. This will return you to the Report Options window (see Figure 7-4 on page 4 of this section).
6. Click on the Print button. The report window appears (see Figure 7-6 on page 7 of this section). Use the scroll bars to review information within the report.

NOTE: If you need to change the orientation between portrait or landscape, click on the button on the top tool bar. Select the orientation needed and click on the OK *button. The button will not appear on the top tool bar if you have not selected it in the Window Style Options as shown on Figure 7-5 on page 6 of this section.*

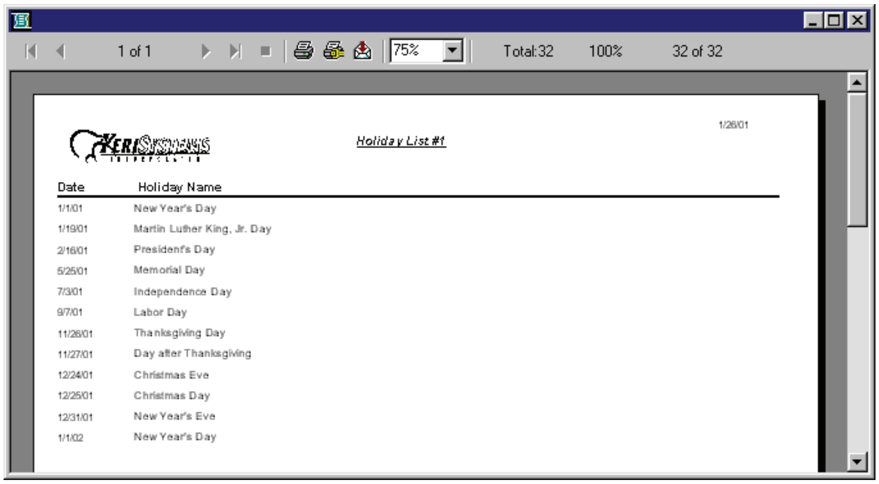


Figure 7-6: View Formatted Report Window

7. Click on the Done button at the completion of the report generation.

1.2.2 Save Report to File

1. To save the formatted report to file, click on the on the left side of the "Report" field in the Report Options window and select Export the report (see Figure 7-4 on page 4 of this section).
2. To select when you want to save the report, click on the on the right side of the "Report" field and select "right now" (see Figure 7-4 on page 4 of this section).
3. In the central field, click on the button. The Export window will appear (see Figure 7-7).

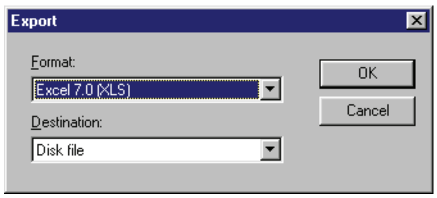


Figure 7-7: Export Window

4. Click on the below the "Format" field to choose the format in which you would like to save the report.
5. Click on the below the "Destination" field to choose the where you want to save the file.
6. Click on the button.

NOTE: There are 32 different format options to choose from. It is not feasible to demonstrate each and every one in this guide. Depending on your selections in the Format and Destination fields, you will see different windows where you will need to make further choices regarding the report style, type, and destination.

7. When all your selections have been made, you will be returned to the Report Options window (see Figure 7-4 on page 4 of this section).
8. To save the report, click on the button. The file is saved according to your specifications.
9. Click on the button at the completion of the report generation.

1.2.3 Print Report

1. To print the formatted report, click on the  on the left side of the "Report" field in the Report Options window and select Print the report to a printer (see Figure 7-4 on page 4 of this section).
2. To select when you want to print the report, click on the  on the right side of the "Report" field. For this example, select "right now" (see Figure 7-4 on page 4 of this section).

NOTE: When you have selected the "at a specific time" option, use the "Time" and "Date" field scrolls to determine when the report will be printed.

3. In the central field, click on the  button. The Print window will appear (see Figure 7-8).

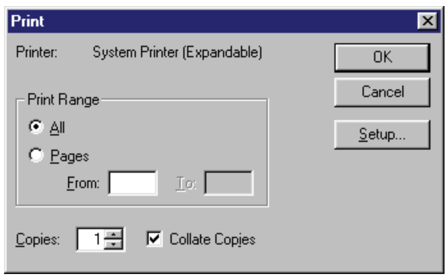


Figure 7-8: Print Window

4. Click on the  button. The Print Setup window appears (see Figure 7-9).

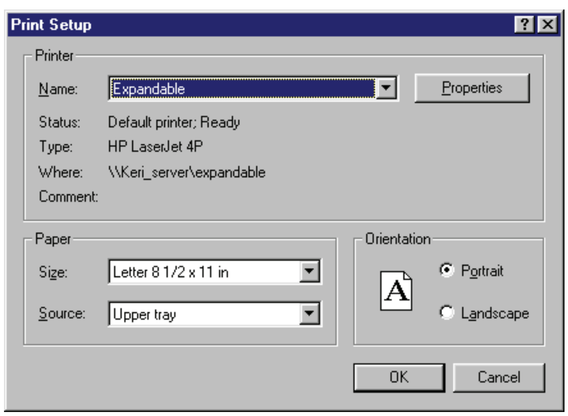


Figure 7-9: Print Setup Window

5. In the "Printer Name" field, click on the  to select the printer.

6. Once you have made your printer selection, click on the  buttons until you return to the Report Options window (see Figure 7-4 on page 4 of this section).
7. When you are ready to print the report, click on the  button.
8. Click on the  button at the completion of the report generation.

*NOTE: If you have selected a time other than right now to print the report, the Print Options window will minimize and remain on your desktop tool bar until it prints. Your computer **must** remain on until the report prints. If you turn off the computer, the print report request will be canceled.*

2.0 Quick Search Event Report

To create a quick search event report, click on the Reports ⇒ Searchable Events pull-down menu option. The Event Reports window appears (see Figure 7-10).

NOTE: For information on finding video clips related to Doors events, see the Visions Quick Start Guide (P/N 01974-001). For information on finding video clips related to Doors EntraGuard events, see the section for *"EntraGuard" on page 1 in section 10*.

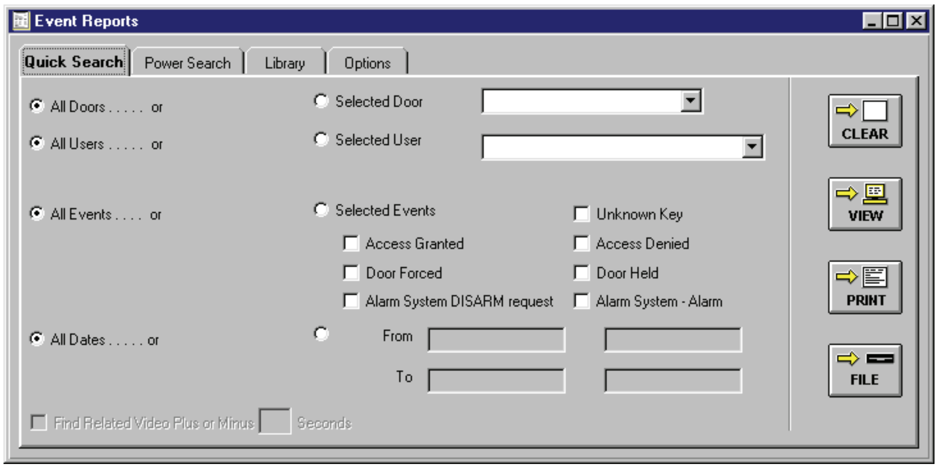
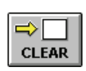


Figure 7-10: Quick Search Event Reports Window

2.1 Clear all Fields

The clear button clears all data fields and returns all search selection parameters to default values (which shows all events).

NOTE: This is a destructive operation, removing all entered search parameters.

1. To clear all fields, click on the  button. To verify the clear operation should be performed, a confirmation window appears (see Figure 7-11).

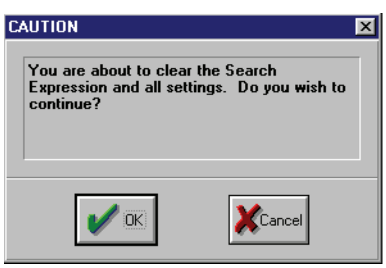


Figure 7-11: Clear Search Fields Confirmation Window

2. Click on the  button.

2.2 Select Doors

The doors radio buttons allow an operator to select if event information should be reported for all doors or for just one selected door.

1. To select all doors, click on the **All Doors** radio button (the default value, see Figure 7-10 on page 11 of this section).
2. To select one door, click on the **Selected Door** radio button. A list of all available doors appears in the window (see Figure 7-12).

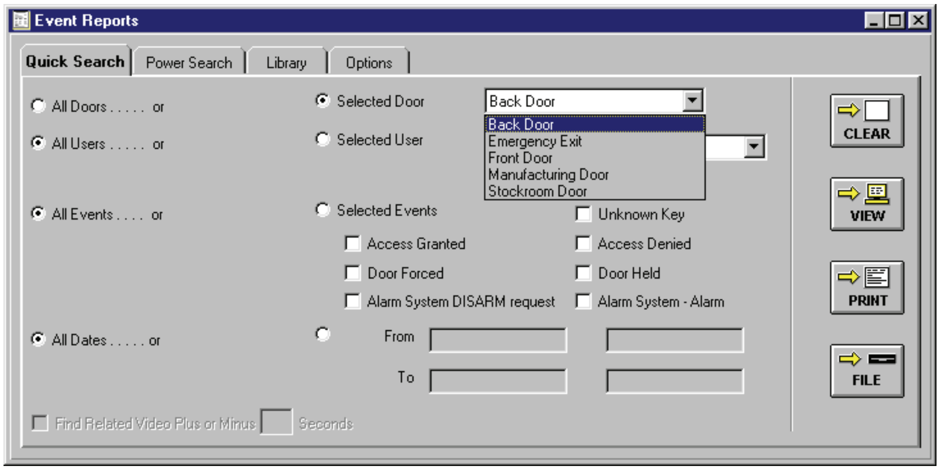


Figure 7-12: Available Door List

3. Scroll through the list and locate the door for which a report is desired. Click on that door name and it will be entered into the selected door field (see Figure 7-13).

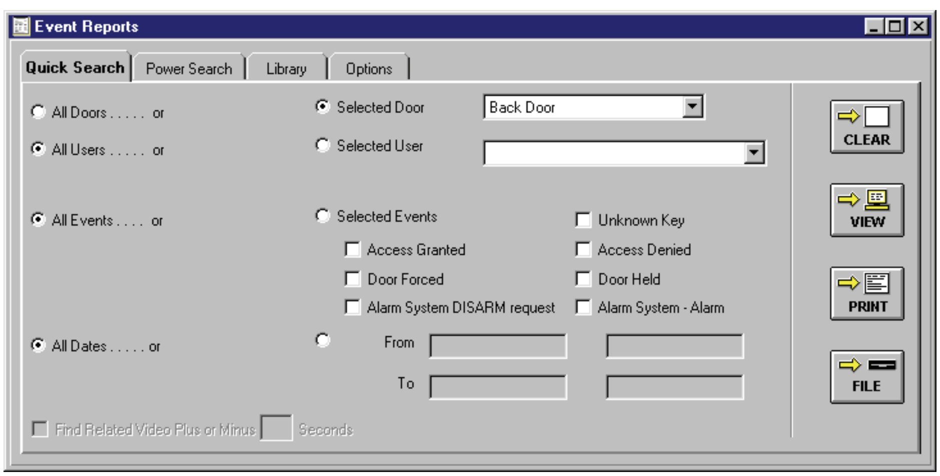


Figure 7-13: Selected Door

4. To select a different door, click on the  box and the list of available doors will reappear.

2.3 Select Users

The users radio buttons allow an operator to select if event information should be reported for all users or for just one selected user.

1. To select all users, click on the **All Users** radio button (the default value, see Figure 7-10 on page 11 of this section).
2. To select one user, click on the **Selected User** radio button. A list of all available users appears in the window (see Figure 7-14).

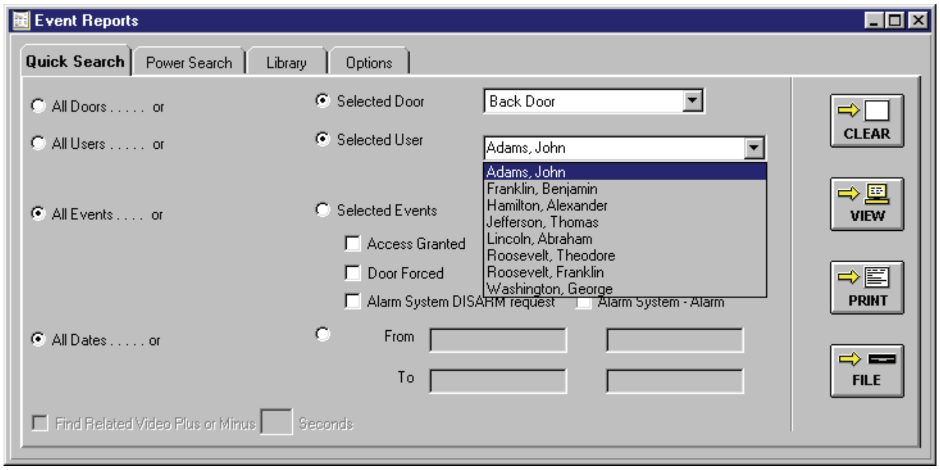


Figure 7-14: Available Users List

3. Scroll through the list and locate the user for which a report is desired. Click on that user name and it will be entered into the selected user field (see Figure 7-15).

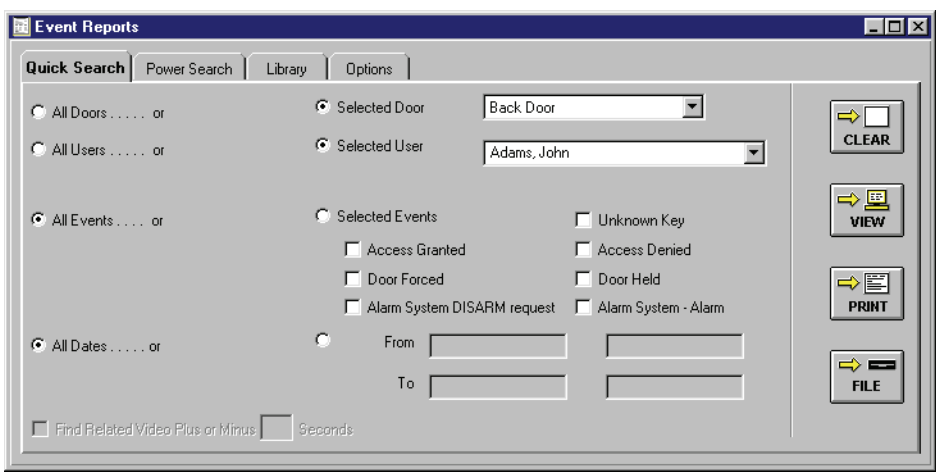


Figure 7-15: Selected User

4. To select a different user, click on the  box and the list of available users will reappear.

NOTE: If a user name has not been assigned to a card enrolled in the system, the card's internal number will be displayed in the Selected User list.

2.4 Select Events

The events radio buttons allow an operator to select if event information should be reported for all events or for just events selected from the provided list.

1. To select all events, click on the **All Events** radio button (the default value, see Figure 7-10 on page 11 of this section).
2. To select events from the provided list, click on the **Selected Event** radio button. Beneath the selected events radio button is a list of the seven most commonly requested event report parameters.
3. To select any or all of these seven events for event reporting, click on the check box beside the event. When a check mark appears in the box, the event is selected. If the box is empty, the event is not selected (see Figure 7-16).

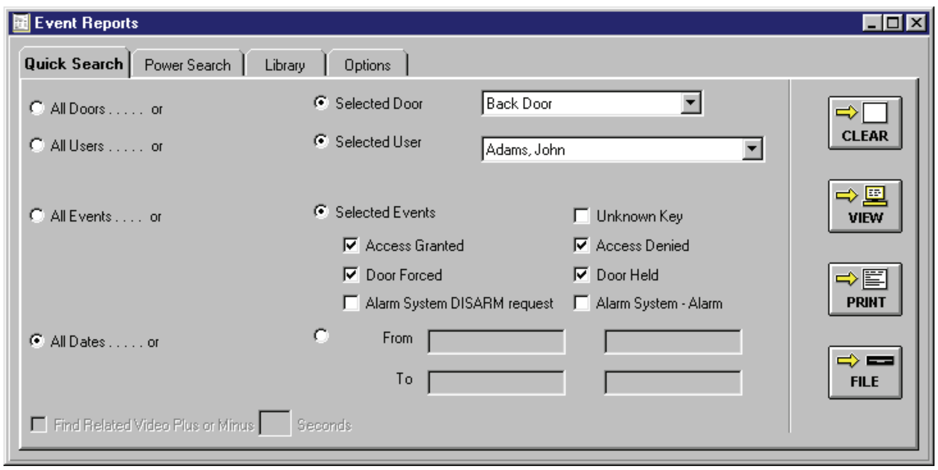


Figure 7-16: Selected Events

2.5 Select Dates and Times

The dates radio buttons allow an operator to select if event information should be reported for all dates or just between selected days and times.

1. To select all dates, click on the **All Dates** radio button (the default value, see Figure 7-10 on page 11 of this section). This will show all information available on the criteria selected above without any date filter.
2. To select dates between specific days and times, click on the **From. . . To** radio button. The default is for the **From. . . To** fields to display today's date.
3. In the From field, enter the beginning date and time for reporting events. If the time field is left at the default of 00:00:00, the events from the beginning of the day (Midnight) are reported. For example, to report on events beginning on July 4, 2000 at 17:00 hours, double-click in the From date field and type **07/04/2000**. Double-click in the From time field and type **17:00:00** (see Figure 7-17).
4. In the To field, enter the ending date and time for reporting events. If the time field is left at the default of 23:59:59, the events from the entire day are reported. For example, to report on events ending on July 5, 2000 at 08:00 hours, double-click in the To date field and type **07/05/2000**. Double-click in the To time field and type **08:00:00** (see Figure 7-17).

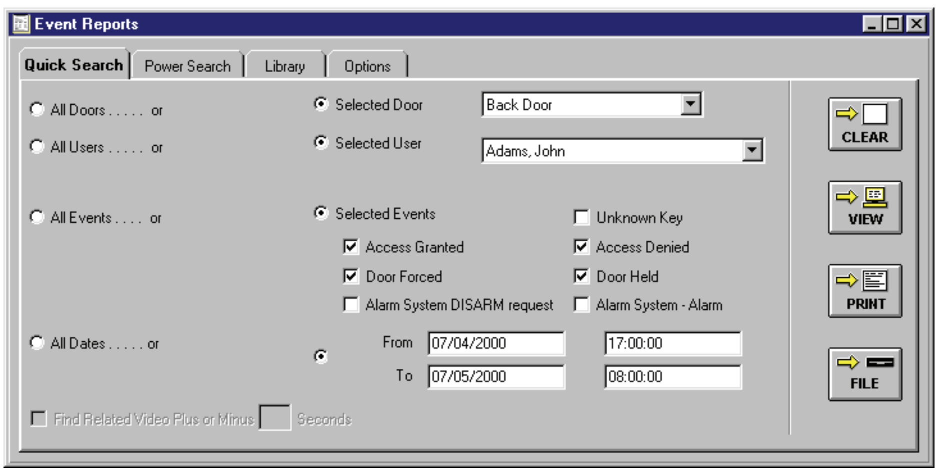


Figure 7-17: Selected Dates and Times

2.6 Generate Report Output

Once a report search criteria has been set, there are three formats for generating the event report output.

- view the report on the computer
- print the report
- save the report to an ASCII text file

2.6.1 View Report on Screen

1. To view the event report on the computer, click on the 

button. All event data will be reviewed and sorted based on the criteria in the Quick Search window.
2. If there was no data that meets the search criteria, an empty report warning window appears (see Figure 7-18). Click on the 

button and modify the search criteria in the Quick Search window.

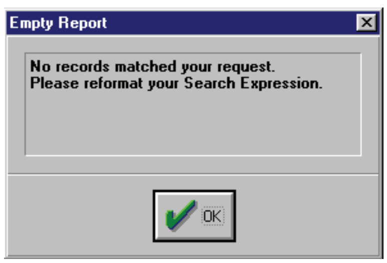


Figure 7-18: Empty Report Window

3. If the search was successful, a success window appears (see Figure 7-19).

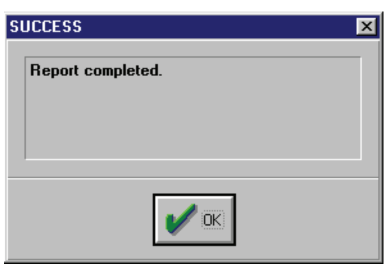


Figure 7-19: Successful Report Window

4. Click on the 

button and the report window appears (see Figure 7-20 on page 17 of this section). Use the scroll bars to review the information within the report.

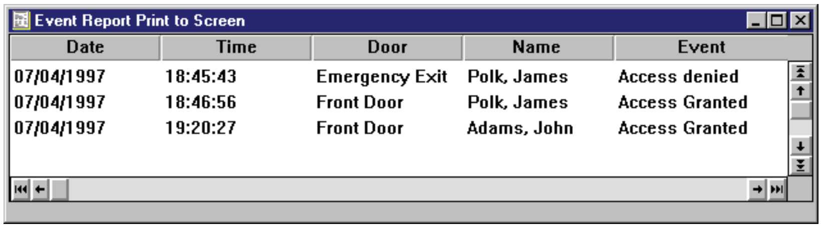


Figure 7-20: View Report Window

NOTE: No more than 32,000 events can be viewed on screen for any given report search. If greater than 32,000 events meet the search criteria for that report, any events over the 32,000 limit will not be shown.

2.6.2 Print Report

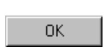
1. To print the event report, click on the  button. All event data will be reviewed and sorted based on the criteria in the Quick Search window.
2. If there was no data that meets the search criteria, an empty report warning window appears (see Figure 7-18 on page 16 of this section). Click on the  button and modify the search criteria in the Quick Search window.
3. If the search was successful, a *Windows* Print Window appears. Enter any printer parameters as needed (print parameters vary based on the type of printer installed and on the *Windows* setup parameters).
4. Click on the  button and the report is printed.

NOTE: No more than 64 pages of events can be printed for any given report search. If greater than 64 pages of events meet the search criteria for that report, any events over the 64 page limit will not be shown.

2.6.3 Save Report to File

1. To save the event report to an ASCII file on the computer, click on the  button. All event data will be reviewed and sorted based on the criteria in the Quick Start window.
2. If there was no data that meets the search criteria, an empty report warning window appears (see Figure 7-18 on page 16 of this section). Click on the OK button and modify the search criteria in the Quick Search window.
3. If the search was successful, a *Windows* File Save window appears.
4. In the File Name field, enter a descriptive file name. For example, for an event report of back door access it could be named “Back Door Access.txt”.

NOTE: The Windows operating system allows up to 255 characters for the file name, but has a 3 character limitation for the extension.

5. In the Folders field, locate the folder where the report file should be saved (the default is to save it in “c:\kerisys\doors32 vX.XX”).
6. Click on the  button and the report is saved.

3.0 Power Search Event Reports

Power search event reports allow an operator to create custom event reports by creating custom database search expressions. These expressions are created to filter out unwanted information so that the report contains just the desired information.

Power searches are performed on the event file stored on the host computer. The event file is a collection of all events received from all controllers on the access control network. Each event in the file is saved as a string of information. When generating a power search event report, the search expression is applied to each event string and those strings that meet the search expression criteria are added to the report.

NOTE: To successfully create custom database search expressions, the operator must have a basic understanding of Boolean arithmetic. Boolean arithmetic is the tool used to create the custom search expressions. This Users Guide will describe the Boolean operators used in this program, but it cannot teach Boolean arithmetic.

To create a search expression, individual search criteria parameters are defined in the new criterion field (see Figure 7-21) and then are entered into the search expression field to create the complete search expression. There are five individual fields within the new criterion field. A search expression can consist of one Field Type, Operation, and Field Value for a simple data filter. Or it can include Link operators to combine simple expressions into complex expressions, and parenthetical operators to group certain expressions together to perform complex data filtering.

- Field Type – The type of data for which to search.
- Operation – The Boolean operator to use to determine how to include and exclude data.
- Field Value – The value of the Field Type data for which to search.
- Link – Combines Field Type, Operation, and Field Value expressions.
- Group – Parenthetical grouping operators to create complex expressions.

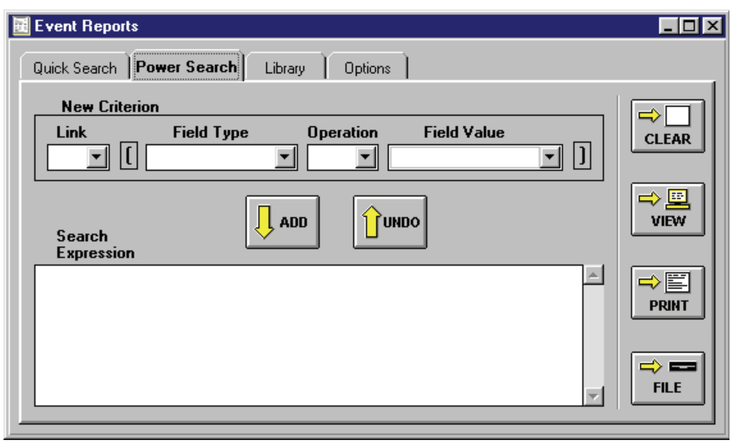


Figure 7-21: Power Search Tab

This section describes the individual fields and values used to create a power search expression, and then it provides an example of creating a complex power search.

3.1 Field Type and Field Value

The **Field Type** identifies the type of event data to be retrieved to generate a report. The items in the Field Type list correspond to information in each event file string. The **Field Value** is the specific value of the event data to be retrieved to generate a report.

There are five Field Types; each type having a specific set of Field Values.

- **Event** sets the search criteria to retrieve events (such as Access Denied, Door Forced, or Request to Exit). When Event is selected, a pull-down list of all possible events appears for selection in the Value Field (see “Message Text String Definitions” on page 7 in section 5 for descriptions of all possible events).
- **Time** sets the search criteria to retrieve all events that occurred at a specific time. When Time is selected, the specific time for which to search must be entered in the Value Field.
- **Date** sets the search criteria to retrieve all events that occurred on a specific date. When Date is selected, a specific date for which to search must be entered in the Value Field.
- **Door** sets the search criteria to retrieve all events that occurred at a specific door. When Door is selected, a pull-down list of all available doors in the access control network appears for selection in the Value Field.
- **Name** sets the search criteria to retrieve all events that occurred to a specific user. When Name is selected, a pull-down list of all available users in the access control network appears for selection in the Value Field.
- **Zone/User/Device** (Alarm Control) sets the search criteria to retrieve all events that occurred to a specific zone, user, or device.
    - When Zone is selected, a pull-down list of all available alarm control zones in the access control network appears for selection in the Value Field.
    - When User is selected, a pull-down list of all available users in the access control network with Alarm Control priveleges appears for selection in the Value Field.
    - When Device is selected, a pull-down list of all available alarm control devices in the access controll network appears for selection in the Value Field.
- **Partition Number** (Alarm Control) sets the search criteria to retrieve all events that occurred within a specified partition. When Partition is selected, a pull-down list of all available alarm control partitions in the access control network appears for selection in the Value Field. If no partitions have been set up, then the Value Field will remain blank.
- **Dept Group** sets the search criteria to retrieve all events that occurred to a specific department group. When a department group is selected, a pull-down list of all available department groups in the access control network appears for selection in the Value Field. If no department groups have been entered in the User database, the Value Field will appear blank.

3.2 Boolean Operators

Boolean operators determine how the data being searched will be filtered to locate the data specifically requested by the report. There are six Boolean operators.

- Equal To (=)
- Greater Than or Equal To (>=)
- Less Than or Equal To (<=)
- Greater Than (>)
- Less Than (<)
- Not Equal To (<>)

Equal To (=)

As a report is being generated, a search expression using the Equal To operator examines each data string in the event database, searching for data strings that meet the search expression's Field Type.

If the Field Type is a match, the Field Value in the data string is then compared with the Field Value in the search expression. If the value in the data string is **equal to** the value in the expression, the data string is included in the report; if not, it is excluded from the report.

For example, if the Field Type is set to Date and the Field Value is set to 07/04/1997, the report would only include events that occurred on July 4, 1997 (see Figure 7-22). Events that occurred on any other date would be excluded from the report.



Figure 7-22: Equal To Criterion Sample

Greater Than or Equal To (>=)

As a report is being generated, a search expression using the Greater Than or Equal To operator examines each data string in the event database, searching for data strings that meet the search expression's Field Type.

If the Field Type is a match, the Field Value in the data string is then compared with the Field Value in the search expression. If the value in the data string is **greater than or equal to** the value in the expression, the data string is included in the report; if not, it is excluded from the report.

For example, if the Field Type is set to Date and the Field Value is set to 07/04/1997, the report would only include events that occurred on or after July 4, 1997 (see Figure 7-23). Events that occurred before July 4, 1997 would be excluded from the report.

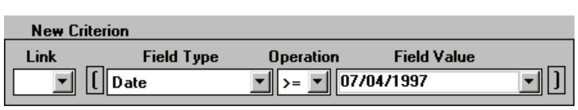


Figure 7-23: Greater Than or Equal To Criterion Sample

Less Than or Equal To (<=)

As a report is being generated, a search expression using the Less Than or Equal To operator examines each data string in the event database, searching for data strings that meet the search expression's Field Type.

If the Field Type is a match, the Field Value in the data string is then compared with the Field Value in the search expression. If the value in the data string is **less than or equal to** the value in the expression, the data string is included in the report; if not, it is excluded from the report.

For example, if the Field Type is set to Date and the Field Value is set to 07/04/1997, the report would only include events that occurred on or before July 4, 1997 (see Figure 7-24). Events that occurred after July 4, 1997 would be excluded from the report.

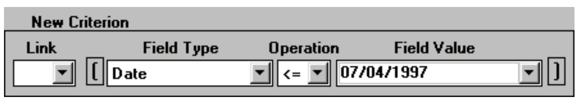


Figure 7-24: Less Than or Equal To Criterion Sample

Greater Than Operator (>)

As a report is being generated, a search expression using the Greater Than operator examines each data string in the event database, searching for data strings that meet the search expression's Field Type.

If the Field Type is a match, the Field Value in the data string is then compared with the Field Value in the search expression. If the value in the data string is **greater than** the value in the expression, the data string is included in the report; if not, it is excluded from the report.

For example, if the Field Type is set to Date and the Field Value is set to 07/04/1997, the report would only include events that occurred after July 4, 1997 (see Figure 7-25). Events that occurred on or before July 4, 1997 would be excluded from the report.

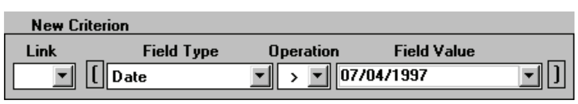


Figure 7-25: Greater Than Criterion Sample

Less Than Operator (<)

As a report is being generated, a search expression using the Less Than operator examines each data string in the event database, searching for data strings that meet the search expression's Field Type.

If the Field Type is a match, the Field Value in the data string is then compared with the Field Value in the search expression. If the value in the data string is **less than** the value in the expression, the data string is included in the report; if not, it is excluded from the report.

For example, if the Field Type is set to Date and the Field Value is set to 07/04/1997, the report would only include events that occurred before July 4, 1997. Events that occurred on or after July 4, 1997 would be excluded from the report (see Figure 7-26).



Figure 7-26: Less Than Criterion Sample

Not Equal To operator (<>)

As a report is being generated, a search expression using the Not Equal To operator examines each data string in the event database, searching for data strings that meet the search expression's Field Type.

If the Field Type is a match, the Field Value in the data string is then compared with the Field Value in the search expression. If the value in the data string is **not equal to** the value in the expression, the data string is included in the report; if not, it is excluded from the report.

For example, if the Field Type is set to Date and the Field Value is set to 07/04/1997, the report would only include events that did not occur on July 4, 1997. Events that occurred on July 4, 1997 would be excluded from the report (see Figure 7-27).

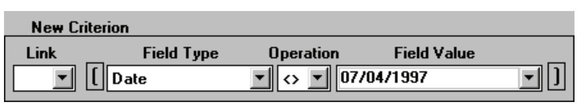


Figure 7-27: Not Equal To Criterion Sample

3.3 Boolean Links

Boolean links are used to link simple expressions together to create complex expressions where several conditions must be met before data should be included in a report. Since a link cannot be done until there are at least two expressions, the link field does not become active until at least one expression has been entered into the Search Expression field. There are four types of Boolean links used by the *Doors* program.

- AND
- OR
- AND...NOT
- OR...NOT

AND
An AND link allows operator to link two search expressions together so that as event data is being reviewed for a report the data must meet the criteria in both expressions to be included in the report.

For example, an AND link consisting of (Date>=07/04/1998@00:00 **AND** Date<=07/04/1998@23:59) **AND** Event=Access Denied would filter event data and create a report that displays only the Access Denied events that occurred on July 7, 1998. The search expression generated by this link appears in Figure 7-28.

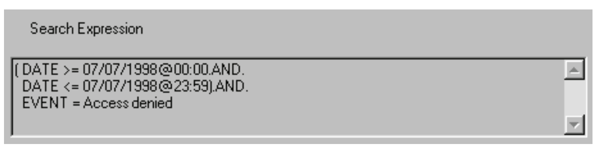


Figure 7-28: AND Boolean Link Sample

OR
An OR link allows operator to link two search expressions together so that as event data is being reviewed for a report the data must meet the criteria in either expression to be included in the report.

For example, an OR link consisting of (Date>=12/24/1998@00:00 AND Date<=12/24/1998@23:59) **OR** (Date>=12/25/1998@00:00 AND Date<=12/25/1998@23:59) would filter event data and create a report that displays all events that occurred on either December 24, 1998 or December 25, 1998. The search expression generated by this link appears in Figure 7-29.

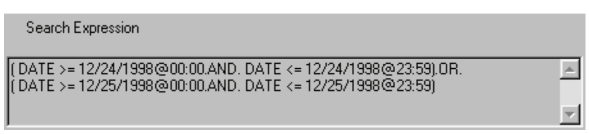


Figure 7-29: OR Boolean Link Sample

AND...NOT
An AND...NOT link allows operator to link a search expression so that as event data is being reviewed for a report the data that meets the AND..NOT criteria is excluded from the report.

For example, an AND...NOT link consisting of (Door=Controller 1/Door1) **AND...NOT** Event=Access Granted would filter event data and create a report of all events that occurred at Controller1/ Door 1 excluding all Access Granted events from the report. The search expression generated by this link appears in Figure 7-30.

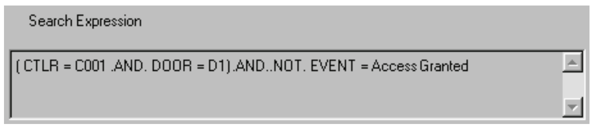


Figure 7-30: AND...NOT Boolean Link Sample

OR...NOT
An OR...NOT link allows operator to link a search expression so that as event data is being reviewed for a report the data that meets the OR...NOT criteria is excluded from the report.

For example, an OR...NOT link consisting of (Door=Controller 1/Door1) **OR...NOT** Event=Access Granted would filter event data and create a report of all events that occurred excluding all Access Granted events that were not at Controller 1/Door1from the report. The search expression generated by this link appears in Figure 7-31.

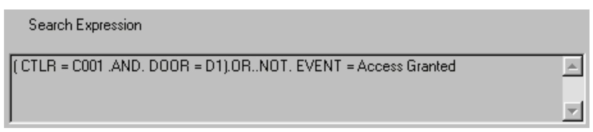


Figure 7-31: OR...NOT Boolean Link Sample

Grouping Operator
Grouping operators allow an operator to combine search expressions to create complex search expressions. Parenthesis are placed around expressions that need to be nested within larger expressions. The expressions with the parenthesis will be evaluated as a group and the results will be applied to the larger expression outside the parenthesis.

For example, a complex expression consisting of (Event=Request To Exit **AND** DATE=07/04/1998) **AND** (Event=Door Opened **AND** DATE=07/04/1998) would filter event data and create a report that only consisted of Request to Exit and Door Opened events that occurred on July 4, 1998. The search expression generated by this link appears in Figure 7-32.

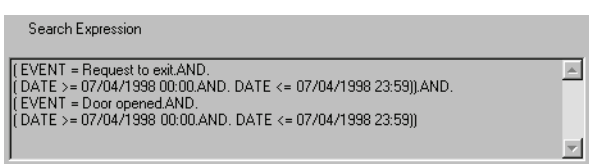


Figure 7-32: Grouping Operator Sample

Search Expression Field

Once a search expression has been defined in the New Criterion field, it must be added to the Search Expression field. Searches are performed from the expressions in the Search Expression field.

1. To add a search expression to the Search Expression field, simply click on the 

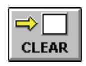
button (see Figure 7-21 on page 18 of this section). The expression in the New Criterion field is entered into the Search Expression field in the format used by the search/sort algorithm.

2. To delete a search expression from the Search Expression field, click on the 

button (see Figure 7-21 on page 18 of this section). The last expression added to the search expression field will be removed.

Clear all Fields

Before creating a search expression, all data fields should be cleared to ensure no "left-over" search parameters from previous queries affect the new entry. The clear button clears all data fields and returns all search selection parameters to default values (which shows all events).

1. To clear all fields, click on the 

button. To verify the clear operation should be performed, a confirmation window appears (see Figure 7-11 on page 11 of this section).

2. Click on the 

button.

3.4 Power Search Example

An operator needs to create a search expression that generates a report that meets the following criteria.

- any Access Denied or Door Forced Open events
- occurring at either the Front Door or Back Door
- on July 5, 1998
- during 00:00 hours to 08:00 hours (Midnight to 8 A.M.)

Perform the following steps to set the search expression to search only for Access Denied or Door Forced Open events.

1. Click on the  button.
2. Click on the  button to accept the clear operation.
3. Click on the [button.
4. Set the Field Type to **Event**.
5. Set the Operation to =.
6. Set the Field Value to **Access Denied**.
7. Click on the  button.
8. Set the Link field to **OR**.
9. Set the Field Type to **Event**.
10. Set the Operation to =.
11. Set the Field Value to **Door Forced Open**.
12. Click on the] button.
13. Click on the  button.

Figure 7-33 displays the search expression to this point.

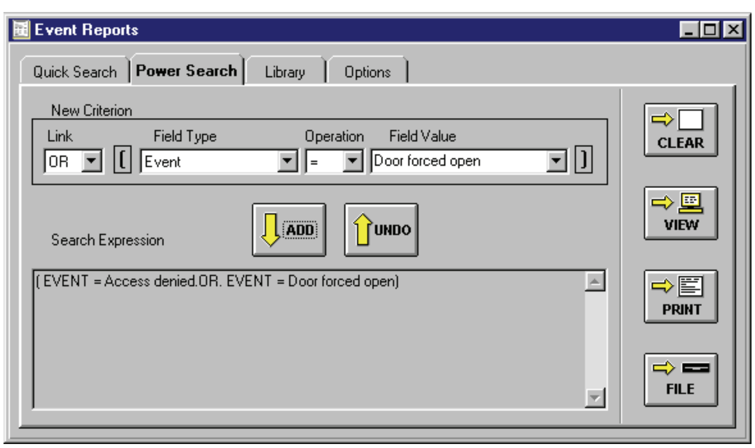


Figure 7-33: Limiting the Search to Access Denied or Door Forced Open Events

Perform the following steps to add the Front Door and Back Door only requirement.

1. Set the Link field to **AND**.
2. Click on the [button.
3. Set the Field Type to **Door**.
4. Set the Operation to =.
5. Set the Field Value to **Default Site, Front Door**.
6. Click on the  button.
7. Set the Link field to **OR**.
8. Set the Field Type to **Door**.
9. Set the Operation to =.
10. Set the Field Value to **Default Site, Back Door**.
11. Click on the] button.
12. Click on the  button.

Figure 7-34 displays the search expression to this point.

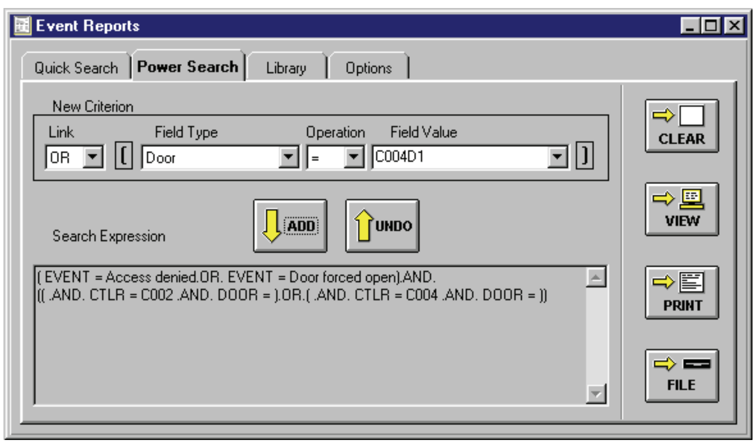


Figure 7-34: Limiting the Search to the Front and Back Doors

Perform the following steps to add the July 5, 1998 requirement.

1. Set the Link field to **AND**.
2. Set the Field Type to **Date**.
3. Set the Operation to =.
4. Set the Field Value to **07/05/1998**.
5. Click on the 

button.

Figure 7-35 displays the search expression to this point.

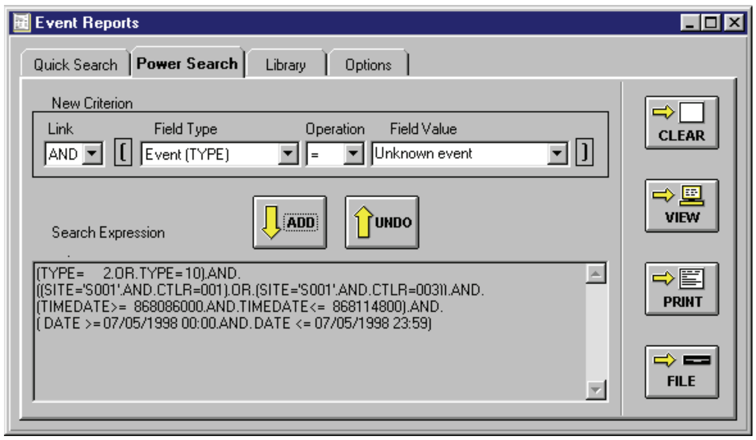


Figure 7-35: Limiting the Search to July 5, 1998

Perform the following steps to add the 00:00 to 08:00 (Midnight to 8 A.M.) requirement.

1. Set the Link field to **AND**.
2. Click on the [button
3. Set the Field Type to **Time**.
4. Set the Operation to >=.
5. Set the Field Value to **00:00**.
6. Click on the 

button.
7. Set the Link field to **AND**.
8. Set the Field Type to **Time**.
9. Set the Operation to <=.
10. Set the Field Value to **08:00**.
11. Click on the] button
12. Click on the 

button.

Figure 7-36 displays the complete search expression.

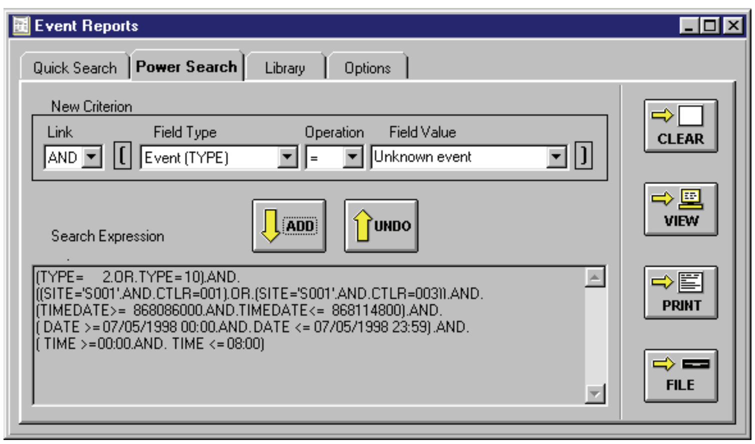


Figure 7-36: Limiting the Search to 00:00 to 08:00 to Complete the Expression

This completes the creation of the power search example. Keri Systems strongly recommends saving power searches, as explained in “Library Tab” on page 30 of this section.

3.5 Generate the Report

The report generation process is identical between Quick Searches and Power Searches. Please refer to “Generate Report Output” on page 16 of this section.

4.0 Library Tab

As operators develop search expressions to generate specific event reports, these expressions can be saved into a library (see Figure 7-37). Once in the library, they can be retrieved and run at specific times, and they can be deleted.

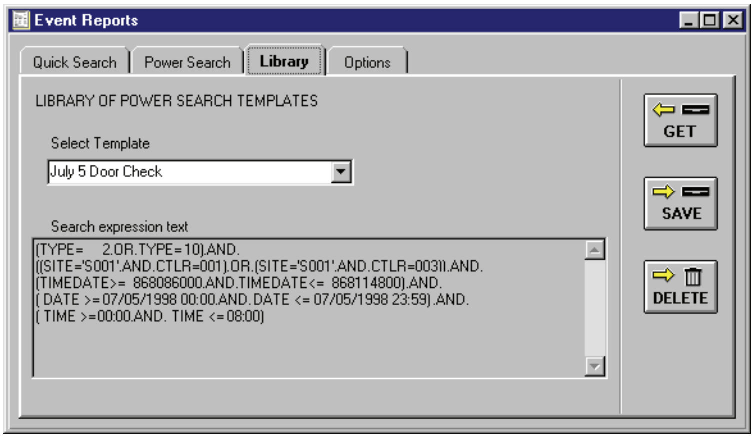


Figure 7-37: Power Search Library Tab

4.1 Save a Search Expression

To save a search expression, a new search expression must have been created under the Power Search tab. This example will save the search expression created in the previous section.

1. To save a search expression, click on the **Library** tab (see Figure 7-37). Verify that the expression to be saved is entered in the “Search Expression” field.
2. Click in the “Select Template” field and enter a descriptive name for the search expression. For example, using the search expression entered in the power search example above, type **July 5 Door Check**.
3. Click on the  button.

4.2 Get a Search Expression

Search expressions that have been saved can be retrieved and run.

1. To retrieve a search expression, click on the **Library** tab (see Figure 7-37 on page 30 of this section).
2. In the Select Template field, click on the  box and a list of available search expressions is displayed (see Figure 7-38).

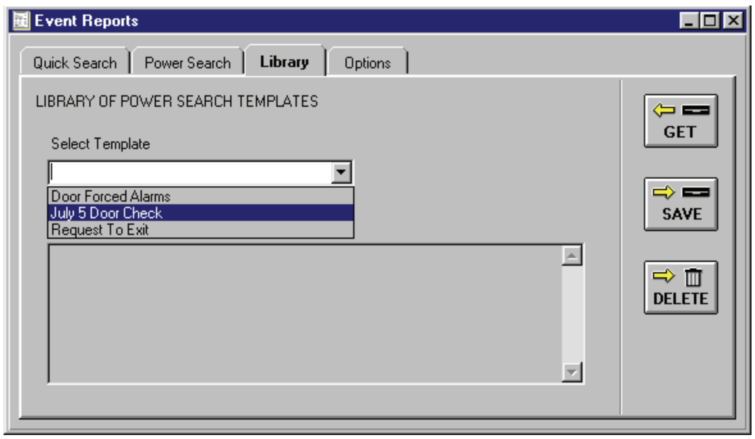


Figure 7-38: List of Saved Search Expressions

3. Scroll up and down the list, locate the desired search expression, and click on it. For example, click on the **July 5 Door Check** template.
4. Click on the  button.
5. The search expression is then displayed in the "Search expression text" field. The operator can review the expression to verify it is the correct one (see Figure 7-37 on page 30 of this section).

4.3 Delete a Search Expression

If a search expression is not needed, an operator can delete it.

1. To delete a search expression, get the search expression to be deleted as described in "Get a Search Expression" as shown above.
2. Click on the  button and the contents of the Select Template and Search Expression fields are deleted, removing this search expression from the library.

NOTE: Use the delete feature with caution. Once a search expression is deleted it cannot be recovered; it must be recreated.

5.0 Options Tab

There are two power search data sorting options available for an operator to choose.
- reverse order of sort
- Card ID/User ID numbers in report file (Time and Attendance)

5.1 Reverse Order of Sort

An operator can choose to reverse the sort order of data in an event report. The default sort order for data is in ascending order, from A to Z or from lowest number to highest number. Reversing the sort order sorts in descending order, from Z to A or from highest number to lowest number.

1. To reverse the sort order, click on the **Options** tab. The Options window appears (see Figure 7-39).

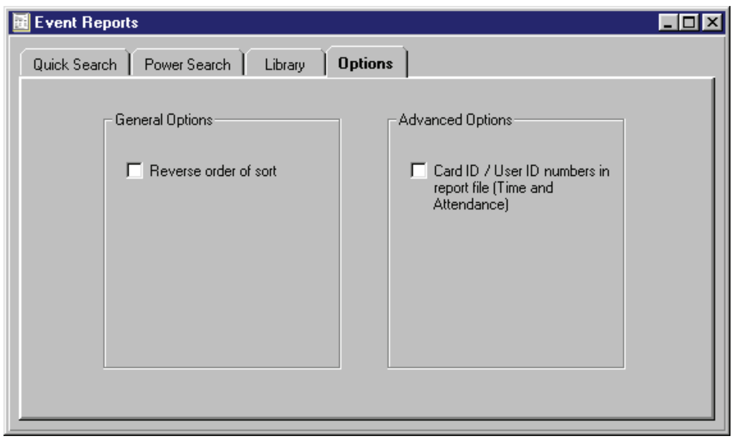


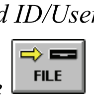
Figure 7-39: Power Search Options Tab

2. To reverse the sort order, in the General Options field, click on the “Reverse order of sort” check box. If the box has a check mark, the report sorts in descending order, from Z to A or from highest number to lowest number.
3. If the box does not have a check mark, the report sorts in ascending order, from A to Z or from lowest number to highest number.

5.2 Save Card ID/User ID Numbers in the Report File

An operator can choose to use card ID/User ID numbers instead of user names in an event report file. The default is set for user names. When you use the card ID/User ID numbers, the user’s name is replaced with the card or User ID number.

1. Click on the Options tab. The Options window appears (see Figure 7-39 on page 32 of this section).
2. To use the card ID/User ID number, in the Advanced Options field, click on the “Card ID/User ID numbers in report file” box; a check mark appears. With a check mark in the box, the report replaces the user’s name with the card ID/User ID numbers.
3. To use the user’s name, in the Advanced Options field, click on the “Card ID/User ID numbers in report file” box; the check mark disappears. With no check mark in the box, the report uses the user’s name.

NOTE: The use of Card ID/User ID numbers instead of user names is only available when you save the report to File using the 

button.

Section 8

Multiple Sites

The multiple site feature allows a number of access control networks to be managed by the *Doors* program; via modem, TCP/IP, or direct connect. The host computer and each site must have a modem allowing communication between the host computer and each site.

When the sites feature is enabled, a number of windows throughout the *Doors* program are modified and the supporting databases are changed, adding the necessary hooks to support all sites.

New sites can be added one-at-a-time; each independent from each other (no crossover of cardholders between sites), or any combination of interaction between sites can be made (cardholders can be assigned to a number of sites). This section describes the following.

- The process for enabling the remote sites feature.
- The process for entering site related information.
- The process for adding a new site to the system.
- The differences in database entry and program operation.

1.0 Enable Sites

The Multiple Sites: Sites ON check box is used to enable the multiple sites feature (see Figure 8-1).

1. Click on the Setup ⇒ System pull-down menu or click on the  button on the tool bar, then click on the **System Options** tab.
2. If the Sites ON field is not already visible on the System Options tab, click on the 

button. The System Options window will reveal the field for enabling multiple sites (see Figure 8-1).

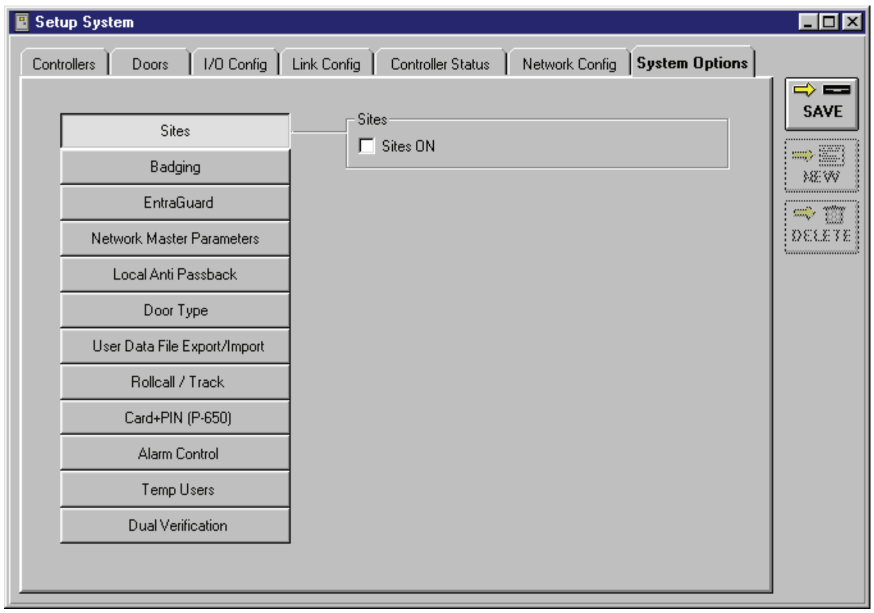


Figure 8-1: System Options Tab - Sites Disabled

3. Click on the **Sites ON** box. A check mark appears in the box. Because the changes required to implement the sites feature make major changes to the *Doors* program and its supporting databases, a confirmation window appears making this reminder (see Figure 8-2).

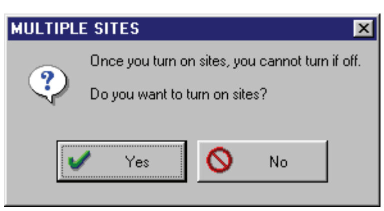
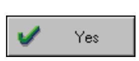


Figure 8-2: Sites On Confirmation Window

4. Click on the 

button. A Save window appears (see Figure 8-3 on page 4 of this section). The conversion to Sites mode will not actually be made until it is saved into the program databases.

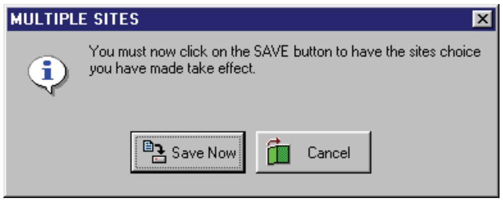


Figure 8-3: Save Sites Choice Window

5. Click on the  button and the conversion to Sites mode automatically occurs.
6. Changes are made in both the System Options and Network Configuration tabs, removing the configuration parameter fields for the remote modem. The modem parameter fields have been moved to a new Sites tab and reformatted to allow for parameter entry for each site (see Figure 8-4).

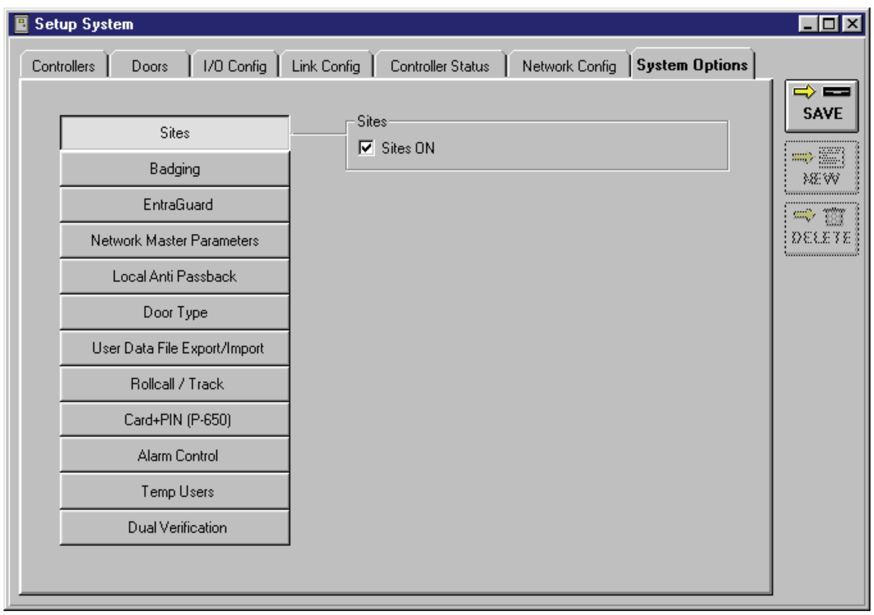


Figure 8-4: System Options Tab - Sites Enabled

7. Now update the access control network with the new information. Click on the  button on the tool bar (for details on the update process refer to “Update the Network” on page 35 in section 5).

The Sites tab is now added to the Setup/System window. Information for the original site is automatically entered in the appropriate locations in the sites database found under the Sites tab (see Figure 8-5 and Figure 8-6).

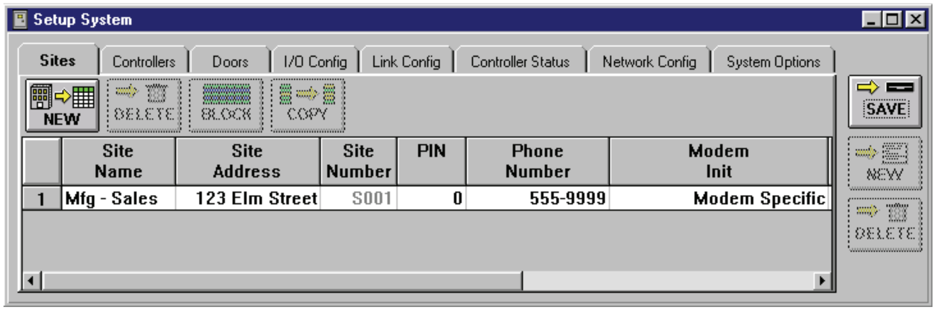


Figure 8-5: Site Information for the Original Site - Part 1

NOTE: If a site is configured for TCP/IP communications, the "Phone Number" column header changes to "TCP/IP Address" and the "Modem Init" column header changes to "Remote Port Number".

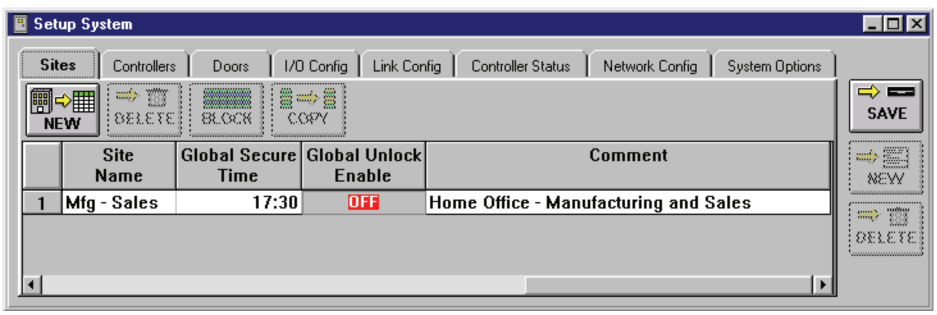


Figure 8-6: Site Information for the Original Site - Part 2

2.0 Adding a New Site

Perform the following to add a new site to the spreadsheet.

1. Click on the Setup ⇒ System pull-down menu or click on the  button on the tool bar, then click on the **Sites** tab.
2. Click on the 

site button. A new row appears on the Sites spreadsheet (see Figure 8-7). Information for the new site is added as shown in “Enter Site Configuration Information” on page 7 of this section.

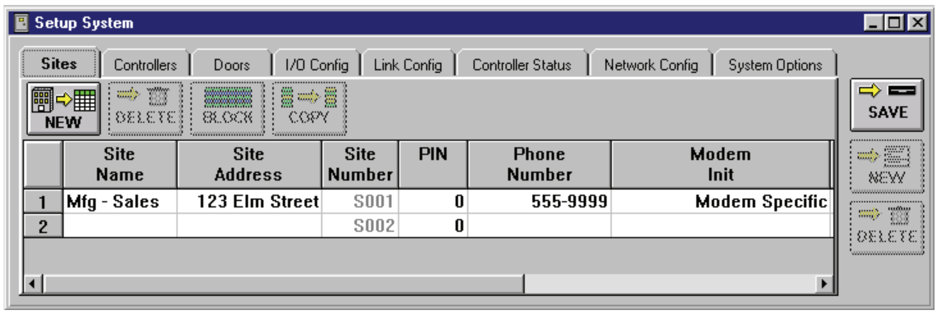


Figure 8-7: Adding a New Site

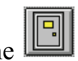
3.0 Enter Site Configuration Information

The Sites tab allows an operator to configure the communication parameters and provide identification information for the individual sites.

The following operations are performed in this section.

- assign a site name
- enter a site address
- enter a site PIN
- enter a site's modem phone number or TCP/IP address
- enter a modem's initialization string or remote port number
- enter a global secure time
- enable the global unlock feature for a site
- enter a comment regarding a site

To enter the Sites tab:

1. Click on the Setup ⇒ System pull-down menu or click on the  button on the tool bar. The following window will appear, including the new tab: Sites.
2. Click on the **Sites** tab. The Sites window appears (see Figure 8-7 on page 6 of this section).

3.1 Assign a Site Name

The site name field allows an operator to assign a descriptive, identifying name to a site in the access control network. When monitoring system activity, or generating and reviewing event reports, it can be easier to follow a string of events if the site associated with the events has a descriptive name.

1. Click on the "Site Name" cell for the site to be named.
2. Type a descriptive name for the site. For example, the new site is for a parts warehouse; type **Warehouse** (see Figure 8-8 on page 9 of this section).

3.2 Enter the Site Address

The site address field allows an operator to store the address of a site in the access control network.

1. Click on the "Site Address" cell for the site.
2. Type in the address for the site. For example, the parts warehouse is located on 987 Oak Avenue; type **987 Oak Avenue** (see Figure 8-8 on page 9 of this section).

3.3 Site Number

The site number is assigned by the *Doors* program. It helps the program track database information by site. It is not editable by the operator.

3.4 Site Personal Identification Number (PIN)

The site PIN field allows an operator to assign a "password" number to a site in the access control network. Once a PIN has been assigned to a site, it is stored in the software and is visible each time you open the Network Configuration tab. The PIN number is an extra security measure to prevent anyone with the same software from gaining unauthorized access to any given site

1. Click on the "PIN" cell for the site. The default "PIN" is set at 0.
2. Type a four-digit number for the site. For example, the parts warehouse is assigned PIN 1111; type **1111** (see Figure 8-8 on page 9 of this section).

3.5 Site Phone Number or TCP/IP Address

If a site is configured for TCP/IP communications, the "Phone Number" column header changes to "TCP/IP Address".

3.5.1 Site Phone Number

The site phone number field allows an operator to assign the phone number for the modem at a site in the access control network. This is the phone number that the host computer will dial to contact the site.

1. Click on the "Phone Number" cell for the site.
2. Type the phone number for the site. For example, the warehouse's phone number is 555-4567; type **555-4567** (see Figure 8-8 on page 9 of this section).

3.5.2 TCP/IP Address

If you are using a TCP/IP Ethernet connection, you will need to enter the TCP/IP Address. The cell heading will automatically change when you have selected the TCP/IP option in Setup System (see "Ethernet TCP/IP Parameters" on page 5 in section 2).

1. Click on the "TCP/IP Address" cell for the site.
2. Type the address for the LAN-100 unit. The address must be entered in the standard "dot" notation (e.g. 127.0.0.0).

3.6 Site Modem Initialization String or Remote Port Number

If a site is configured for TCP/IP communications, the "Modem Init" column header changes to "Remote Port Number".

3.6.1 Site Modem Initialization

The modem initialization field allows an operator to enter the initialization string for the modem at a site in the access control network. The modem initialization string provides the best operating parameters for the modem. As the modem initialization string differs per modem type and manufacturer, refer to the modem's manual for the initialization string.

1. Click on the "Modem Init" cell for the site.
2. Type the modem initialization string for the site's modem.

3.6.2 Remote Port Number

If you are using a TCP/IP Ethernet connection, you will need to enter the Remote Port Number.

NOTE: The cell heading will continue to read as "Modem Init" until you have selected the TCP/IP option during Setup System (see "Ethernet TCP/IP Parameters" on page 5 in section 2).

1. Click on the "Remote Port Number" cell for the site.
2. The default is set at 3001. For MSS devices, leave the Remote Port Number at the default of 3001. For UDS devices, change the Remote Port Number to 10001. Consult your systems or network administrator if you are unsure which device is in use.

Based on the parameters entered so far, the database for the Mfg - Sales site should look similar to Figure 8-8 on page 9 of this section.

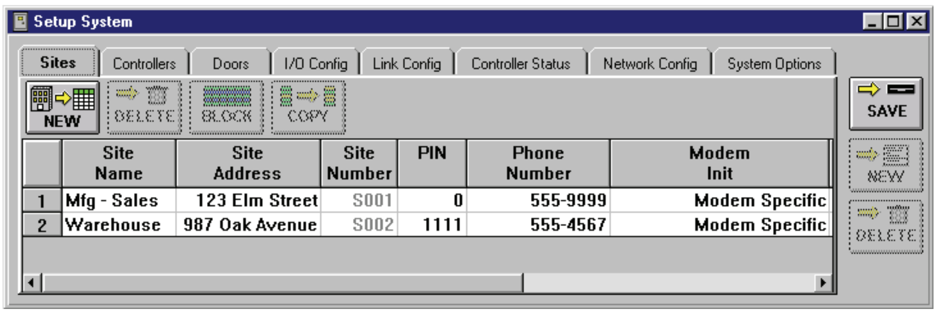


Figure 8-8: Site Configuration Information - Part 1

Depending upon the size of the window displayed on the screen, you might need to use the scroll bar to bring the remaining columns into view (see Figure 8-9).

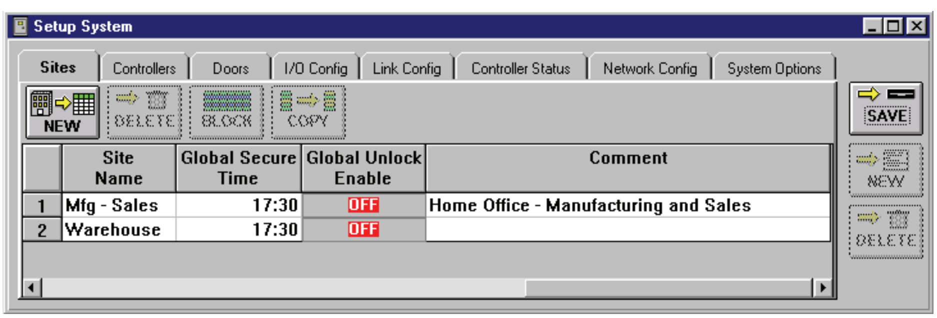


Figure 8-9: Site Configuration Information - Part 2

3.7 Site Global Secure Time

The global secure time field allows an operator to enter a time-of-day when all non-time zone controlled doors in the access control network should be locked. This ensures that regardless of the door status during the day, all non-time zone controlled doors in the access control network are locked at least once a day. The default value for this field is 17:30 (5:30 P.M.).

NOTE: Doors that have an Unlock/Lock Time Zone value of Never are not under automatic time zone control and are eligible to be locked by the global secure time feature.

NOTE: All times are set to a 24-hour clock. For example, 5:30 P.M. is 17:30 under a 24-hour clock.

1. Click on the “Global Secure Time” cell for the site.
2. Type the global secure time for the site. For example, the global secure time for the parts warehouse should be 22:30 hours (10:30 P.M.); type **22:30** (see Figure 8-10 on page 11 of this section).

3.8 Site Global Unlock Enable

The global unlock enable button allows an operator to program the general purpose input on the master controller such that an active signal on the input immediately unlocks all doors on the access control network (refer to the PXL-250 Tiger Controller and SB-293 Technical Reference Manual - P/N 01836-003 or the PXL-250 Quick Start Guide - P/N 01835-002 for general purpose information). The general purpose input is a normally-open input. To activate this input, the input terminals must be closed (shorted together).

NOTE: The global unlock enable feature is not fire marshall approved. Check your local codes for fire safety management.

1. To enable the global unlock input, click on the OFF button. The OFF button toggles to ON (see Figure 8-10 on page 11 of this section).
2. To disable the global unlock input, click on the ON button. The ON button toggles to OFF (see Figure 8-10 on page 11 of this section).

3.9 Site Comment

The site comment field allows an operator to enter a comment regarding the site.

1. Click on the "Comment" cell for the site (see Figure 8-10).
2. Type a brief comment about the site. For example, for the warehouse site type **Parts Warehouse**.

Based on the remaining parameters, the database for the Warehouse site should look similar to Figure 8-10.

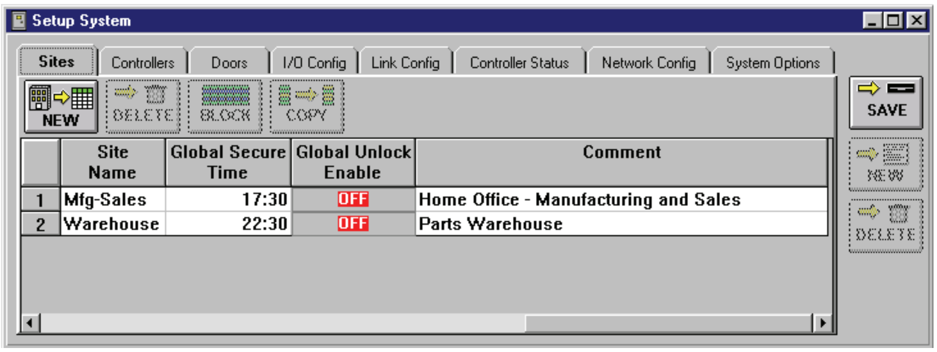


Figure 8-10: Comment Field Information - New Site

3. Once all information is entered, click on the  button. If these changes are not saved before clicking any other button or exiting the system setup window, the data entered is lost and must be re-entered.

4. Now update the access control network with the new information. Click on the  button on the tool bar (for details on the update process refer to "Update the Network" on page 35 in section 5).

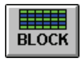
3.10 Block Copying Site Data

The Block and Copy buttons allow an operator to select a data cell for copying to other data cells. This can be helpful when a number of sites have the same information. To minimize data entry, enter the information for the first site and then copy it to the remaining sites. The following fields can be block copied.

- Site Address
- PIN
- Modem Initialization
- Global Secure Time
- Global Unlock Enable
- Comment

In this example, the modem initialization information will be copied from the Manufacturing-Sales site to the Parts Warehouse site.

1. Click on the cell from which data should be copied. In this example, this is the **Modem Init** cell for the Mfg-Sales site.

2. Click on the 

button (see Figure 8-11).

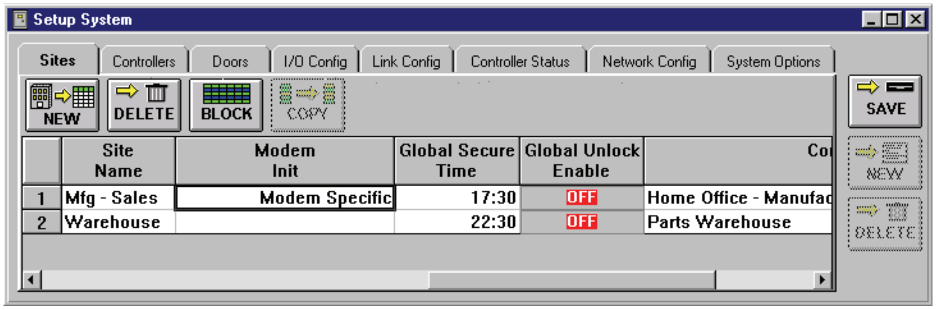


Figure 8-11: Block Selected Data Ready for Copying

3. There are three ways to block select the cells to which data is copied. Use the method you find easiest (see Figure 8-12).

- Click and hold on the first cell to copy and then drag the mouse down to the last cell to copy.
- Click on the first cell, hold the Shift key down, and click on the last cell.
- Hold the Ctrl key down and one-at-a-time click on the cells to be copied. This method is best used when receiving cells are not in sequential order.

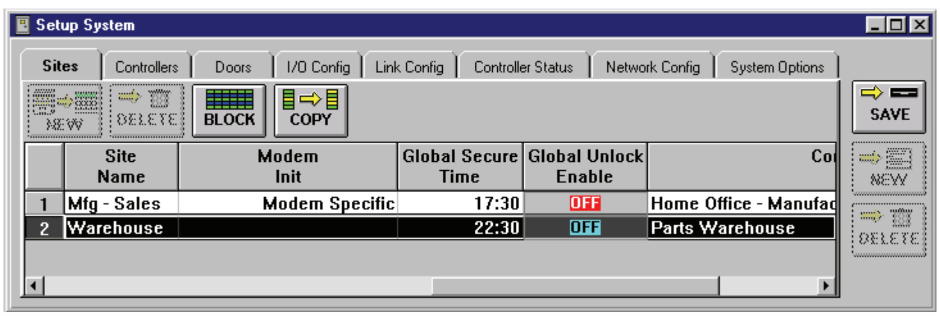


Figure 8-12: Copy Data Rows Selected

Click on the 

button. All data that is able to be copied will be transferred (see Figure 8-13).

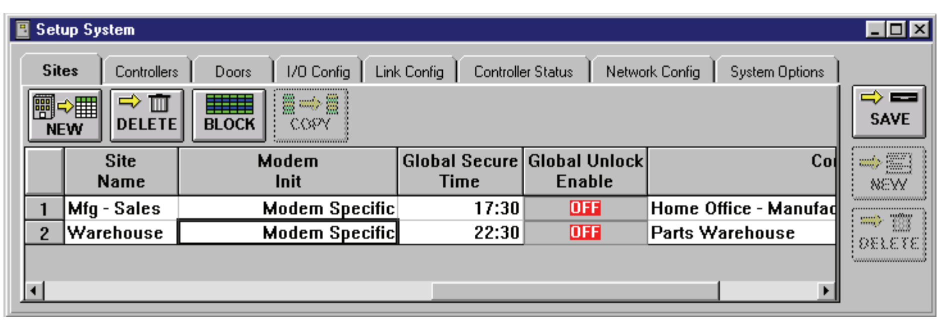


Figure 8-13: Data Copied

4. Click on the 

button. If the copied data is not saved before clicking any other button or exiting the Setup System window, the changes are lost and must be re-entered.

5. Now update the access control network with the new information. Click on the 

button on the tool bar (for details on the update process refer to “Update the Network” on page 35 in section 5).

4.0 Changes in Database Entry and Program Operation

The following database and program operations have minor changes when the multiple sites feature is enabled.

- setup users spreadsheet
- access group wizard
- net update
- select a site button
- quick search reports

4.1 Setup Users Spreadsheet Changes

The Setup Users spreadsheet adds a button that toggles the data displayed in the spreadsheet between displaying user information for one site and displaying information for all sites.

1. To enter the Setup Users spreadsheet click on the Setup ⇒ Users pull-down menu option or click on the  button on the tool bar.
2. Click on the  button on the tool bar to enter spreadsheet mode.
3. When the Setup Users spreadsheet window appears, a new button is displayed beside the original card management buttons.
4. If the 

button is displayed, the user information in the spreadsheet is for the currently selected site only. To **switch** to displaying user information for all sites, click on the 

button.

NOTE: The access group column will only show the access groups associated with the selected site. If you need to change a user's access group from one site to another, you will need to be in all sites mode.

5. If the 

button is displayed, the user information in the spreadsheet is for all sites. To **switch** to displaying user information for the currently selected site only, click on the 

button.
6. Depending upon the size of the user databases, switching between the one-site and all-sites modes can take up to several minutes. A verification window appears before the switch occurs to verify the switch should be performed (see Figure 8-14).

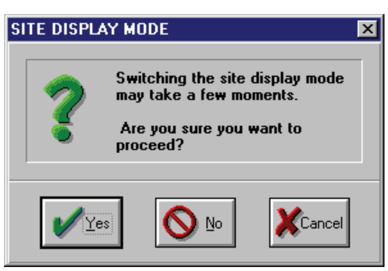


Figure 8-14: Switch Site Display Mode Verification Window

7. Click on the 

button to switch display modes.

4.2 Access Group Changes

The change within the access group wizard adds a select sites window, including site information as a part of the access group. This allows an operator to create new access groups or edit existing access groups to allow access to just one site or to any combination of sites in the access control network. When the select doors window in the access group wizard appears, only those doors associated with the selected sites are displayed.

NOTE: Selected sites can be differentiated from unselected sites by the appearance of the site icon. Selected sites stand out from the window and their site names are written in black text. Unselected sites appear to recede into the window and their names are written in grey text.

4.2.1 For a New Access Group

The Select Sites window appears between the Edit Access Group window and the Select Doors window (see Figure 8-15 on page 15 of this section).

1. To select the sites to be used in an access group, follow the instructions in "Setup Access Groups" on page 44 in section 3, including the following information.
2. After clicking on the 

button and then the 

button in the Edit Access Group window the Select Sites window appears.
3. The Select Sites window displays an icon for every site recognized by the access control network.
4. Click on the icon for any site that should be included in the new access group. For example, click on the Mfg - Sales icon to include only the Mfg - Sales site in the access group (see Figure 8-15).
5. Click on the 

button and the Select Doors window appears. Complete "Create a New Access Group" on page 45 in section 3.

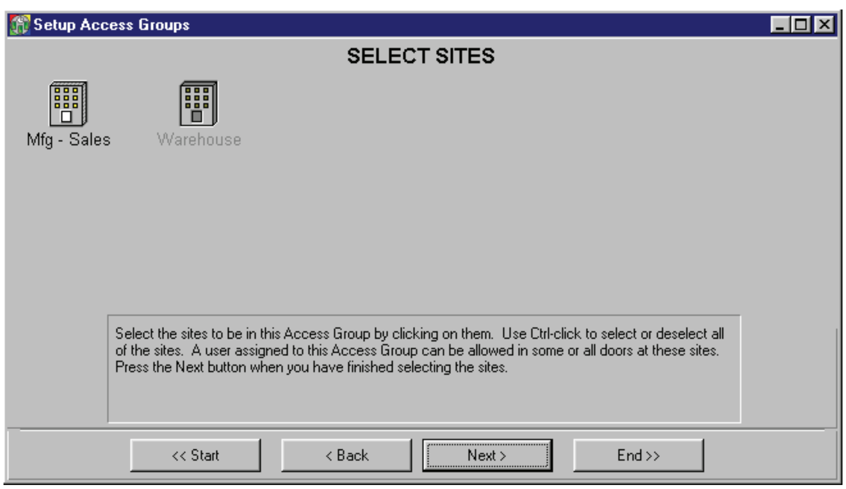


Figure 8-15: Select Sites for Access Groups

4.2.2 For Editing an Access Group

The Select Sites window appears between the Edit Access Group window and the Select Doors window (see Figure 8-15 on page 15 of this section).

1. To select the sites to be used in an access group, follow the instructions in "Setup Access Groups" on page 44 in section 3, but include the following information.
2. After selecting an access group name and clicking on the 

button in the Edit Access Group window the Select Sites window appears.
3. The Select Sites window displays an icon for every site recognized by the access control network.
4. Click on the icon for any site that should be included in the new access group. For example, click on the Mfg - Sales icon to include only the Mfg - Sales site in the access group (see Figure 8-15 on page 15 of this section).
5. Click on the 

button and the Select Doors window appears. Complete "Edit an Existing Access Group" on page 50 in section 3.

4.3 Update Site

On the tool bar, the 

button changes to a 

button. The function is the same, uploading an access control system with all recent changes made to the database. You may upload to all sites from the Update Network window.

1. Click on the 

button on the tool bar. The Update Network window will appear. If changes have been made and the network at any site needs to be updated, the Update Required field will indicate this with a "Yes", and the Skip/Update toggle box under the Smart Update Network field will indicate "Update" (see Figure 8-16).

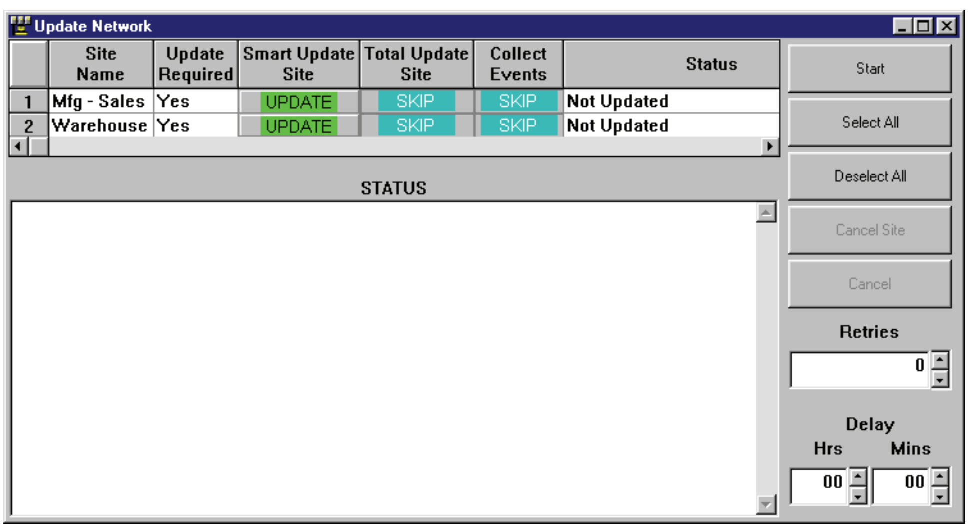


Figure 8-16: Multiple Site Required Network Update

2. Click on the 

button to begin update of the network at each site. The Connect To Site window will appear (see Figure 8-17 on page 17 of this section).

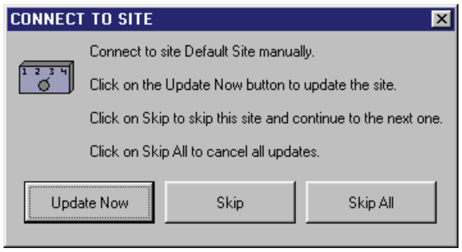


Figure 8-17: Connect To Site Window

3. Click on the  button to begin update of the site designated in the Connect To Site window. If you do not want this site updated at this time, click on the  button. If you want to cancel the update on all sites, click on the  button.
4. If you have chosen to continue with the update, once all parameters are collected, the host computer connects to the access control network. The Network Communication window appears (see Figure 8-18).

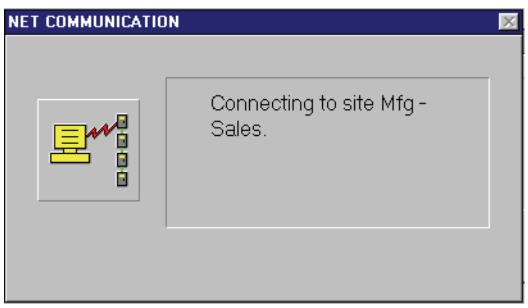


Figure 8-18: Connecting To The Network

5. Once the first site has been updated, the Connect To Site window will appear for the next site (see Figure 8-17). Repeat steps 3 and 4 for each site that is to be updated.
6. When the update process has been completed, the Update Network window should look similar to Figure 8-19 on page 18 of this section.

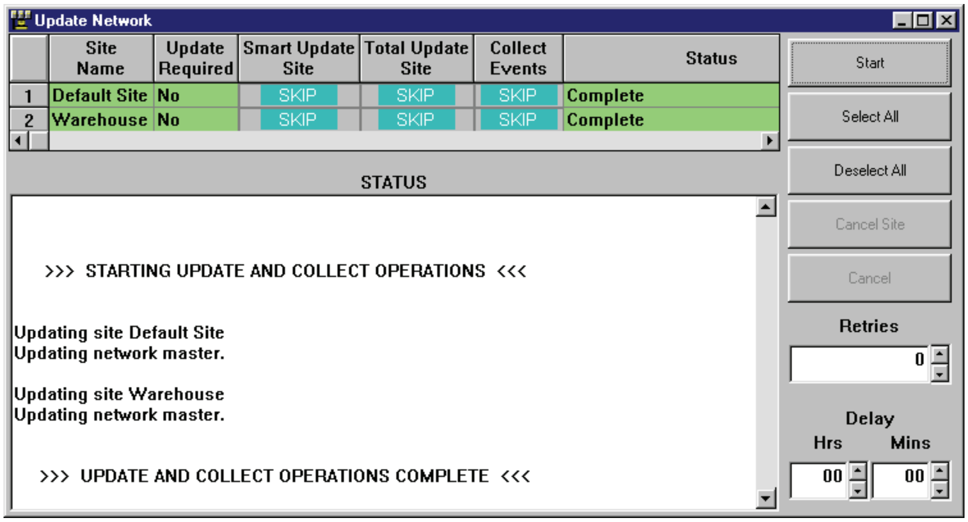
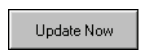


Figure 8-19: Multiple Site Successful Network Update



NOTE: Operator input is required when updating the network while in sites mode. If you attempt to use the delay mode, someone will need to click on the 

button to begin the update process. This is the case even if you are only updating one site.

4.4 Select a Site

A new button is added to the tool bar: 

. Clicking on this button displays a list of all available sites on the access control network, allowing an operator to select a specific site with which to work.

1. Click on the 

button. A window appears with a list of all available sites (see Figure 8-20).

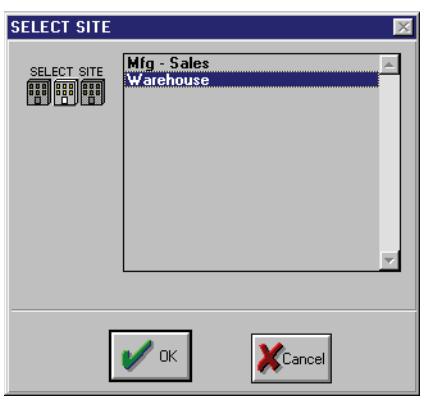


Figure 8-20: Select Site List

2. Scroll up and down the list and select the next site with which to work. Then click on the 

button.
3. The *Doors* software connects with the selected site and loads the program spreadsheets with the data from this site.

4.5 Quick Search Reports by Site

A new All Sites/Selected Site radio button is added to the quick reports feature allowing report data to be sorted by site. Follow the instructions in "Quick Search Event Report" on page 11 in section 7, but include the following information.

The sites radio buttons allow an operator to select if event information should be reported for all sites or for just one selected site.

1. To select all sites, click on the **All Sites** radio button (the default value, see Figure 8-21).

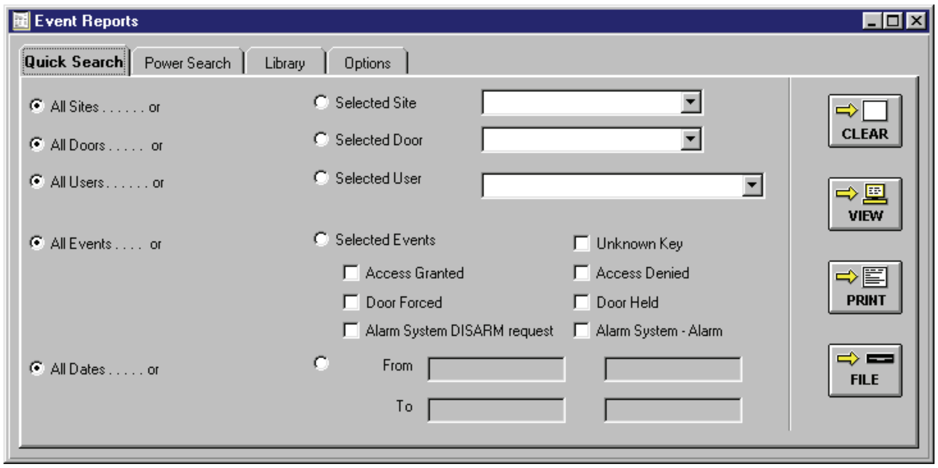


Figure 8-21: Quick Search, All Sites Radio Button

2. To select one site, click on the **Selected Site** radio button. A list of all available sites appears in the window (see Figure 8-22).

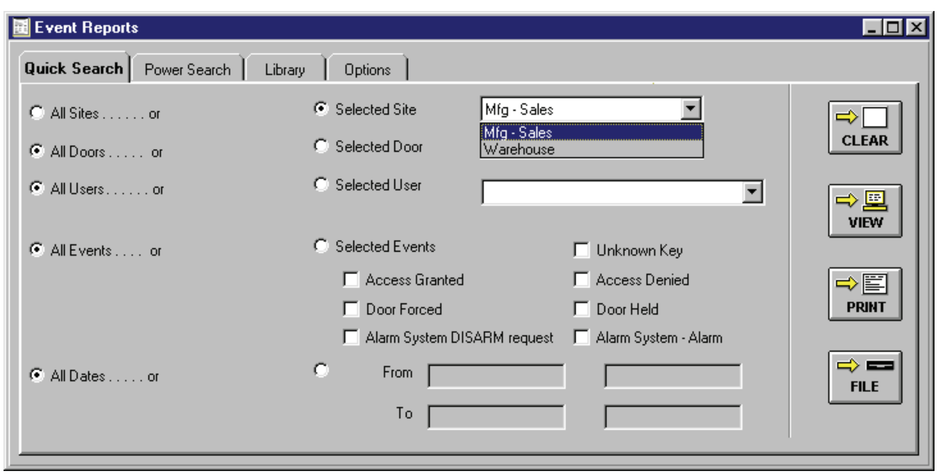


Figure 8-22: Quick Search, Selected Site List

3. Scroll up and down this list and locate the site for event reporting. Click on that site name and it will be entered into the selected site field (see Figure 8-23 on page 20 of this section).

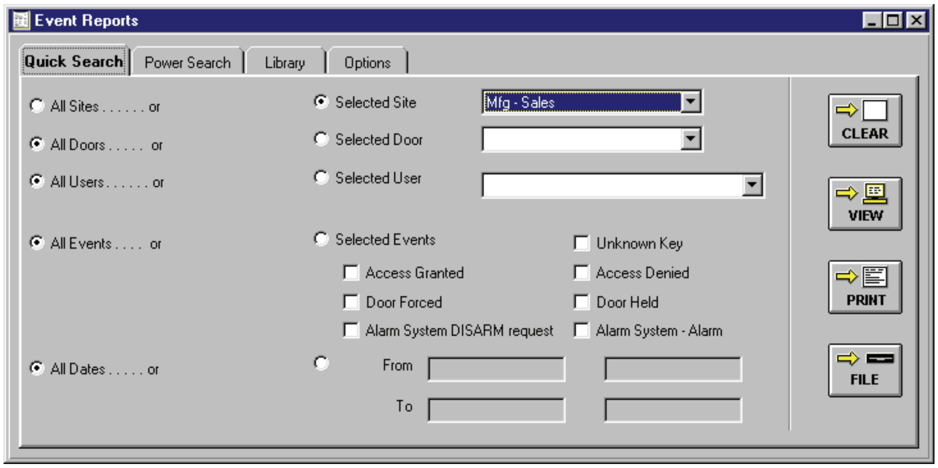


Figure 8-23: Quick Search, Selected Site

4. To change a selected site, click on the ▼ box and the list of available sites will reappear.

4.6 Power Search Reports by Site

A new Field Type/Field Value is added to the power search event reports feature allowing report data to be sorted by site.

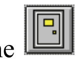
The Site(SITE) Field Type sets the search criteria to retrieve all events that occurred at a specific site. When Site(SITE) is selected, a pull-down list of all available sites in the access control network appears for selection in the Value Field.

5.0 Deleting a Site

If a site becomes unneeded, it can be deleted from the *Doors* databases.

NOTE: As sites are deleted, the database information associated with these sites is removed. Once removed, this information cannot be recovered. If the site needs to be restored, all information associated with the site must be reentered.

In the following example, the Warehouse site will be deleted.

1. Click on the Setup ⇒ System pull-down menu or click on the  button on the tool bar, then click on the **Sites** tab. The following window appears (see Figure 8-24).

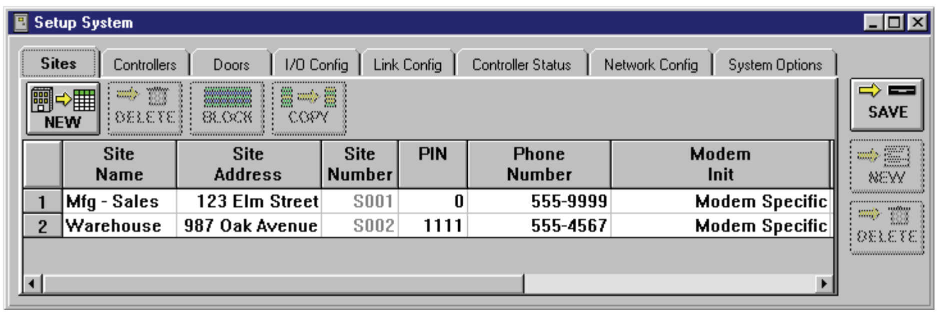


Figure 8-24: Select a Site to Delete

2. Click on the Warehouse Site Name cell. It becomes highlighted to show it has been selected (see Figure 8-25).

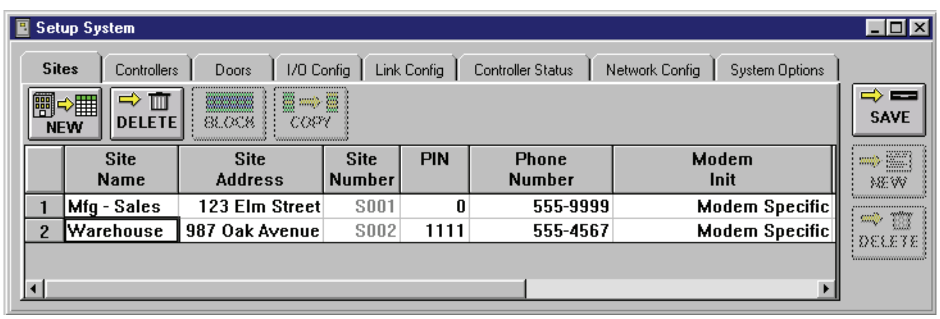


Figure 8-25: Site Selected for Deletion

3. Click on the  button. Since removing a site permanently removes information from databases in the *Doors* program, a confirmation window appears (see Figure 8-26).

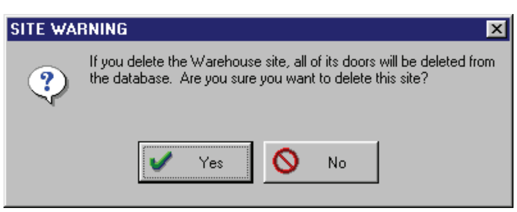


Figure 8-26: Site Deletion Confirmation Window

4. Click on the  button. The site is removed from the *Doors* databases (see Figure 8-27).

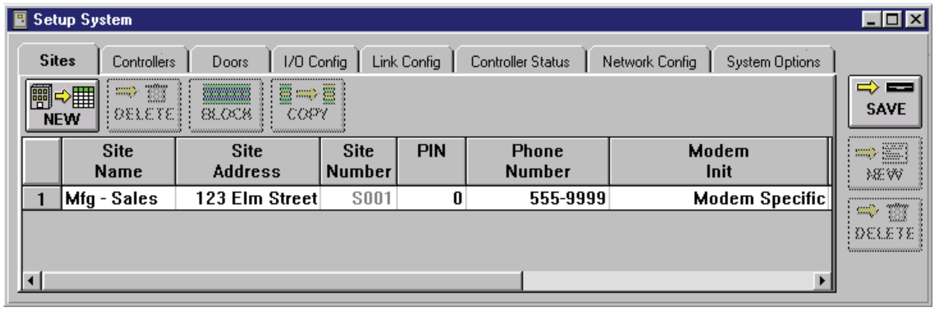


Figure 8-27: Site Deleted

5. Once all sites have been deleted, click on the  button. If these changes are not saved before clicking any other button or exiting the System Setup window, the data entered is lost and must be re-entered.

6. Now update the access control network with the new information. Click on the  button on the tool bar (for details on the update process refer to “Update the Network” on page 35 in section 5).

6.0 Disabling the Multiple Sites Feature

The multiple sites feature can be disabled if necessary, removing all the site related database fields. Before disabling the multiple sites feature, only one site can be active in the database; all other sites must have been deleted per the instructions in “Deleting a Site” on page 21 of this section.

The Multiple Sites: Sites ON check box is used to disable the multiple sites feature (see Figure 8-28). Building off the previous example, the Warehouse site was deleted leaving the Manufacturing-Sales site as the only remaining site. Perform the following steps to disable the multiple sites feature.

1. Click on the Setup ⇒ System pull-down menu or click on the  button on the tool bar, then click on the **System Options** tab. The following window appears (see Figure 8-28).

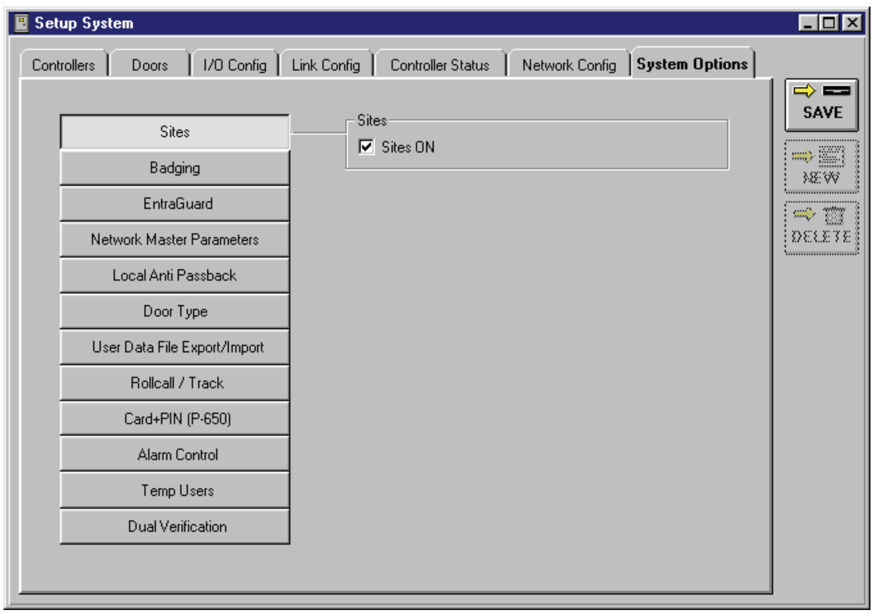


Figure 8-28: System Options Tab - Sites Enabled

2. If the Sites field is not automatically showing, click on the  button. The System Options window will change to reveal the field for enabling multiple sites (see Figure 8-28).

3. Click on the **Sites ON** box. The check mark in the box disappears. Because the changes required to implement the sites feature make major changes to the *Doors* program and its supporting databases, a confirmation window appears making this reminder (see Figure 8-29).

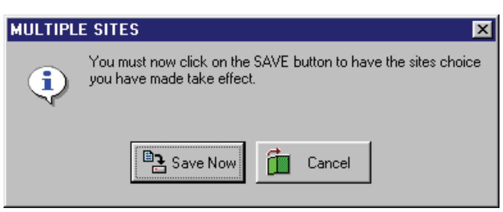


Figure 8-29: Save Sites Choice Window

4. Click the  button. All the site related database fields are now removed, the Sites tab is removed from the setup system window, and the system options window returns to its original state (see Figure 8-30).

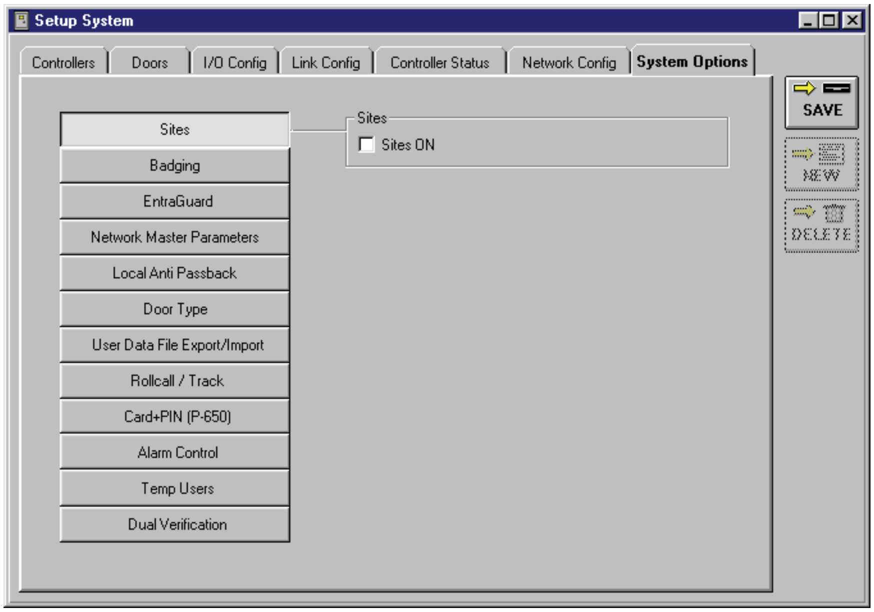


Figure 8-30: System Options Tab - Sites Disabled

Section 9

Photo Badge Management

Document Number 01914-009, Revision 5.2 – September, 2003

Photo Badge Management

Photo ID badge management is integrated in the *Doors* program. An installation option allows Badging to be loaded during the *Doors* software installation process. Refer to the *Doors* Installation Manual (P/N 01821-004) for specific installation information.

Before selecting the Badging option, you must have additional hard disk space in the host computer, beyond what is required by the *Doors* program. This additional space provides storage for the user picture files. The installation program will not install the Badging option if the host computer's hard disk does not meet the following hard disk space requirement.

- 1 to 1,000 users requires an additional 100 MB of hard disk space
- 1,001 to 10,000 users requires an additional 500 MB of hard disk space
- Over 10,000 users requires an additional 1 GB of hard disk space

Badging commands will not appear in the user spreadsheet window until the badging option is enabled, and Badging is not fully functional until a License Code is entered. This License Code is provided by Keri's Customer Support department, and is available for a fee. Even without a License Code, the Badging features can be enabled, tested, and evaluated, but if a badge is printed, it will have the word "SAMPLE" printed across the face of the badge.

Once Badging is enabled, badges are made through a Badging Wizard; a sequential set of windows that guides you through the badge creation process.

Some installations require that Badging operate over a local area network (LAN). Keri's *Doors*/ Badging software can operate over a LAN, but there are a number of limitations that must be considered that affect operation. Please refer to the *Doors* in a Network Environment Application Note (P/N 01867-001) for detailed information on operation over a LAN.

NOTE: If you are using a digital camera as a photo input device, the digital camera must be on Keri Systems' Recommended Peripherals List (P/N 01840-001) to ensure proper operation with the Doors and badging programs. Keri Systems cannot guarantee proper operation with digital cameras not on the Recommended Peripherals List.

1.0 System Contents

A standard Badging system is shipped with the following items.

- Badge Printer
  - Printer Cables – Parallel and USB
  - Power Cable
  - Printer Cleaning Kit
  - Printer Card Cleaning Roller (Installed)
  - Printer Card Hopper (Loader Hopper)
  - Printer Card Hopper (Card Dispenser)
  - Printer Driver CD

- Keri CD Software Package (includes *Doors* software and all product documentation)
  - Serial Loopback Test Plugs
  - MT-10XP Card Kit – blank cards for printer testing
  - *Doors* in a Network Environment Application Note
  - Badging Application Note (this document)

A Keri PC-300 Badging system is shipped with these additional items.

- PC
  - CD-ROM
  - PC Power Cable
  - Monitor
  - Monitor Power Cable
  - Mouse
  - Keyboard
  - Windows Operating System CD

Please verify all of these items are available when you are ready to setup your Badging system.

2.0 System Assembly

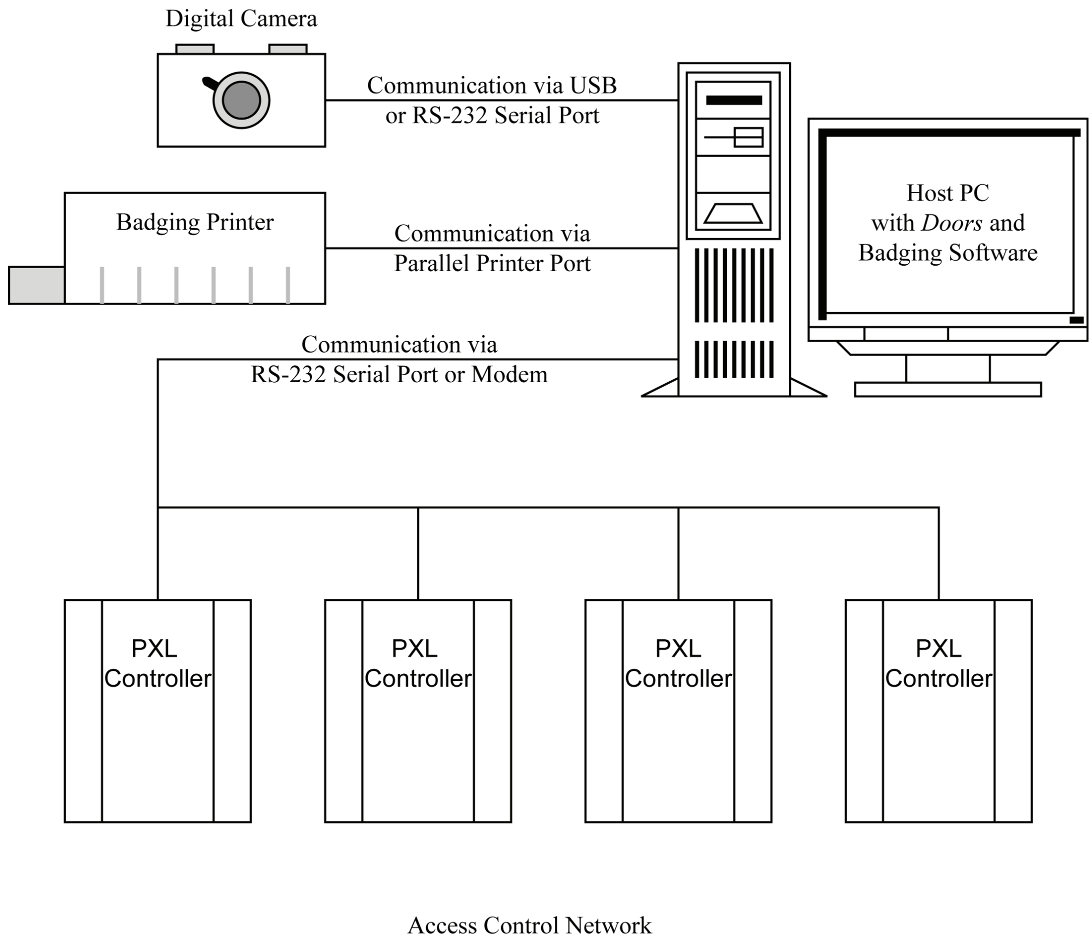


Figure 9-1: Badging System Assembly Diagram

3.0 Badge Templates

GuardDraw is a standalone program provided by ImageWare as a part of the Badging software package. Before producing badges with the *Doors* program, GuardDraw must be used to create a badging template. This template identifies the information fields to be placed on the photo ID badge (both content and location) and it specifies from which *Doors* cardholder database fields this information should be taken. The manual for the GuardDraw program is found on the Keri CD-ROM. Please review the GuardDraw manual for detailed information on how to produce a badging template. The information provided in this section only provides brief summaries of the critical parameters that must be set for *Doors*/Badging operation.

Before creating the template, there are certain parameters in GuardDraw and in the Badging printer driver that must be set to ensure correct communication between the printer and the *Doors*/Badging software package. Once these parameters are set, the template can be created. Once the template is created, *Doors*/Badging is ready to run.

3.1 Badging Printer Preparation

Install the printer drivers for the badging printer on the same system in which *Doors* is running and where the GuardDraw design files are to be created. If the badging printer is not installed correctly, the default Windows printer will be substituted, resulting in an improperly sized template and the inability to use the badging printer.

NOTE: If you upgrade to a new badging printer in the future, be sure to first delete the old printer, but remember the name. Then add the new printer and give it the old name. This ensures that the printer name parameter does not need to be changed within GuardDraw. Once you have set up the badging printer, it is best, if possible, to never change it.

Use the operating system's Control Panel to set the badging printer as the system default printer. This ensures the correct card/printer margins are applied when the GuardDraw program is opened.

Enter the printer's Properties Window and verify that print spooling has been enabled. Click on the Details tab and then the Spool Settings button. Verify the "Spool print jobs so program finishes printing faster" radio button is set. All other spool settings can be left at their default values.

3.2 Set the Path Between Guard/Draw and *Doors*

The GuardDraw program must be correctly pointing to the doors.mdb database file in the *Doors* folder structure. This ensures the cardholder data in *Doors* is readily accessible by GuardDraw.

Perform the following steps to verify the folder pointer.

1. Double-click on the 

icon (on the Windows desktop) to open the GuardDraw program. The GuardDraw main window appears (see Figure 9-2 on page 7 of this section).

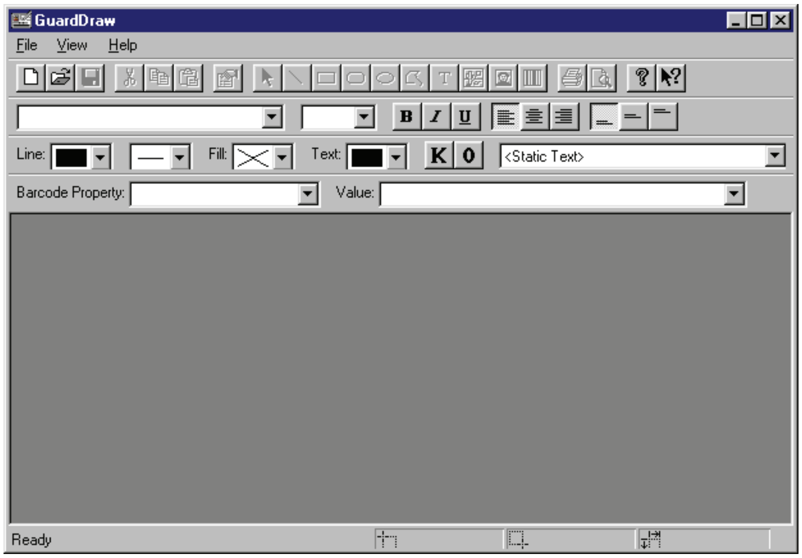


Figure 9-2: GuardDraw Main Window

2 Click on the View ⇒ Options pull-down menu. The General Options window appears (see Figure 9-3).

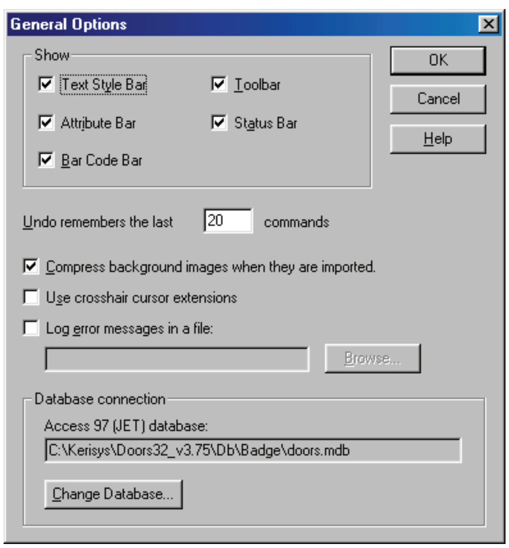


Figure 9-3: GuardDraw General Options

3. At the bottom of the window are the “Database connection” fields. Verify the “Access97 (JET) database” value is set to C:\Kerisys\Doors32vX.X\db\badge\doors.mdb[1] (see Figure 9-3).

4. Click on the OK button.

---

1. This is automatically set to the default *Doors* installation folder. If you have installed the *Doors* program in a different folder, use the Browse... button to locate the doors.mdb file in the folder in which you have installed the *Doors* program. X.X is the revision number of the installed *Doors* software.

3.3 Configuring the Badging Printer

Now the badging printer can be configured for your specific badge requirements.

1. Continuing from Step 4 above, click the File ⇒ New pull-down menu option. This opens a new, blank badge template (see Figure 9-4).

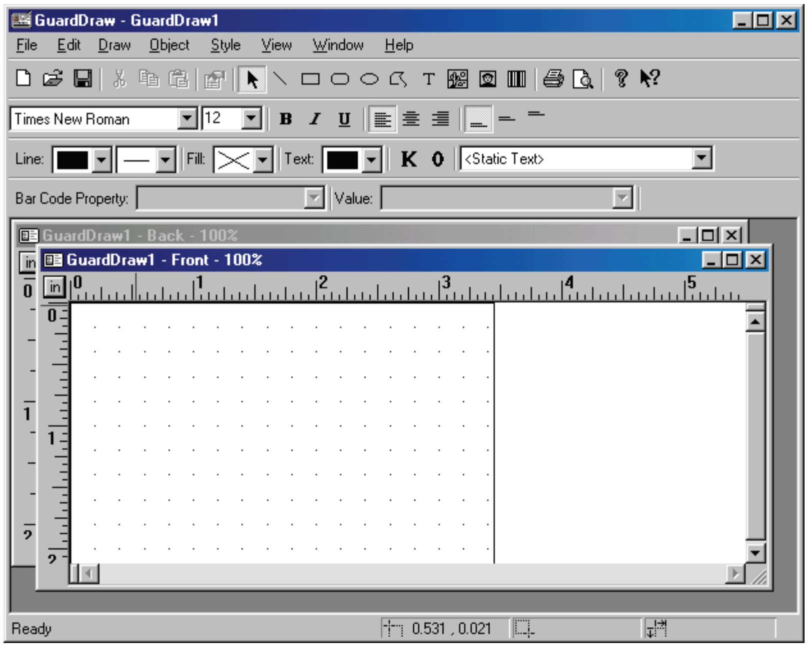


Figure 9-4: Blank Badge Template

2. Click the File ⇒ Print pull-down menu option. The Print window appears (see Figure 9-5).

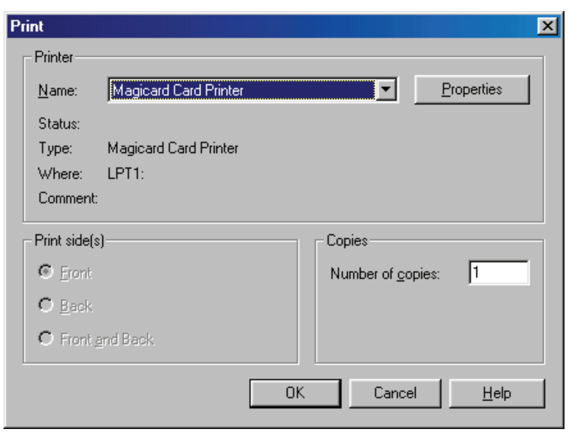


Figure 9-5: The Print Window

3. Click the  at the right side of the “Name” field. A list of available printers appears. Scroll through the list and select the badging printer you have installed.
4. Click the Properties... button. The printer control window appears displaying the printer configuration options beginning with the Printer Tab (see Figure 9-6).

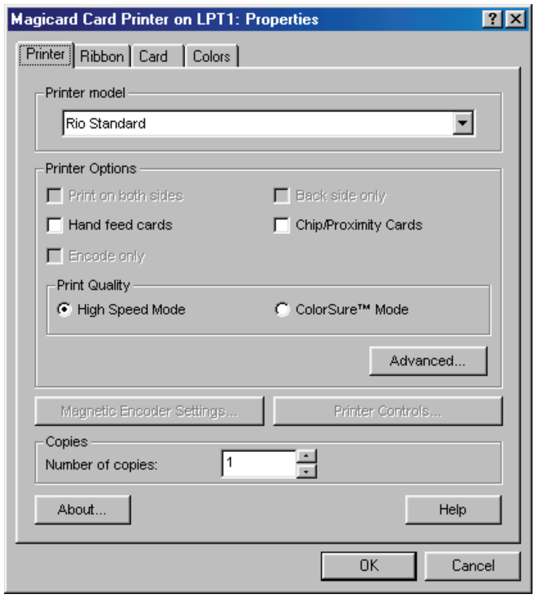


Figure 9-6: Printer Configuration Options – Printer Tab

5. Click the  at the right side of the "Printer model" field. A list of badging printer models appears. Scroll through the list and select the badging printer model you have installed.
6. Based on this selection, certain options are enabled in the "Printer Options" and "Print Quality" fields according to the features within the printer (see Figure 9-6). Of these options, enable those that apply to your printer's capabilities and your printing requirements. For example, if you have a Tango Printer (capable of printing on both sides of a card), you may want to enable the "Print on both sides" feature for two-sided card printing.
7. Click on the Ribbon Tab and a window with printer ribbon options appears (see Figure 9-7).

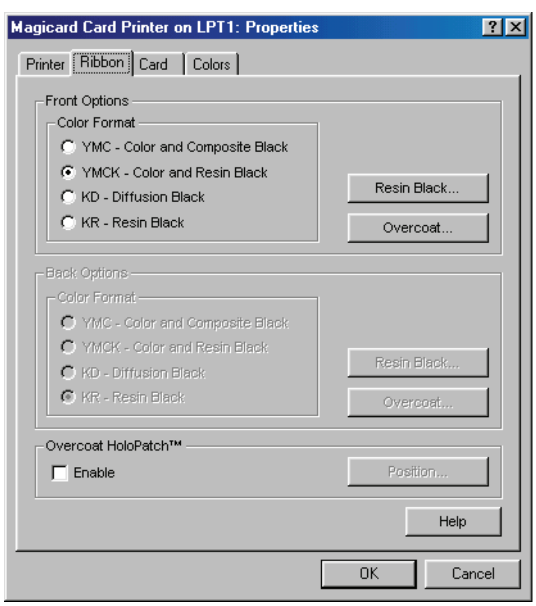


Figure 9-7: Printer Configuration Options – Ribbon Tab

8. For applications using standard ribbons, the default Color Format value of “YMCK - Color and Resin Black” can be left as is. This value should only be changed when using special ribbons that require alternate settings.
9. If desired, you can also enable the optional, clear Overcoat HoloPatch™ feature. When enabled, the 

button becomes active allowing you to select the position of the HoloPatch on the card.
10. Click on the Card Tab and a window with card layout options appears (see Figure 9-8).

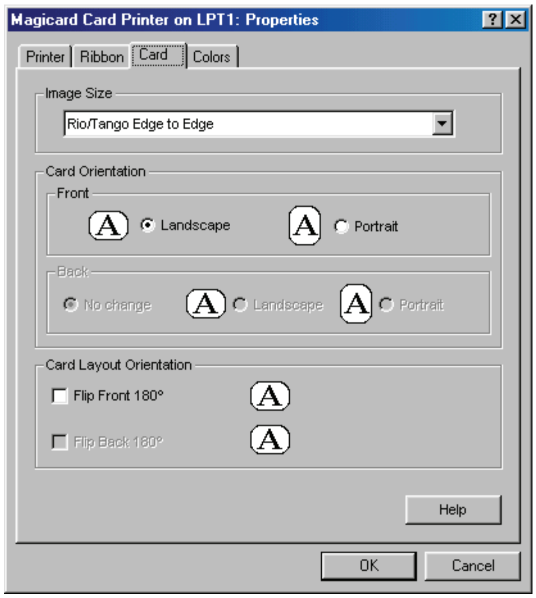


Figure 9-8: Printer Configuration Options – Card Tab

11. The “Image Size” field allows you to define if a template should print cards edge-to-edge or leave a thin white boarder around the edge of the card. Click the  at the right side of the “Printer model” field. A list with these two options appears. Select the option that best suits your needs.
12. In the “Card Orientation” fields, you must select whether you want badges to be printed in Portrait or Landscape format. Click the radio button of your choice to select the card orientation.

*NOTE: Your choice between Portrait or Landscape orientation **must** match what you select under page setup (see Step 9 on page 10).*

13. In the “Card Layout Orientation” field you have the option of rotating the image 180°. To rotate the template, enable the “Flip Front 180°” check box.
14. Click the Colors Tab and a window with color adjustment options appears (see Figure 9-9 on page 11 of this section).

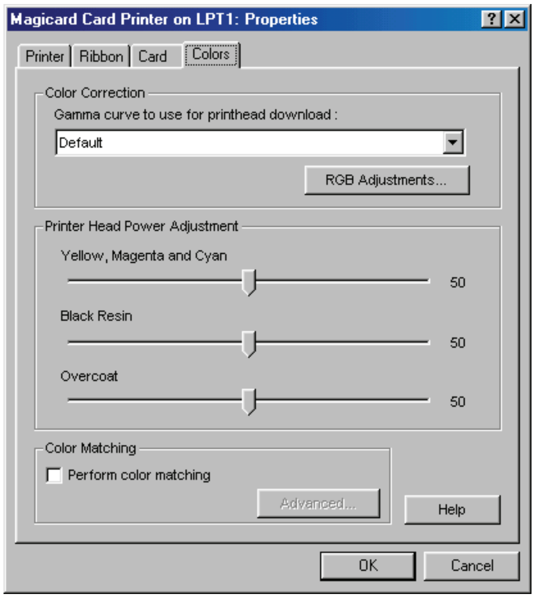


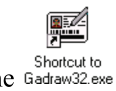
Figure 9-9: Printer Configuration Options – Colors Tab

15. For most applications the default values are acceptable for card printing. These values should only be adjusted if there are printing issues with color or intensity. Please see the GuardDraw manual for detailed information on color adjustment.

3.4 Card Template Design

With the doors.mdb folder pointer set, and the badging printer installed, selected, and configured, you are now ready to create your template.

The GuardDraw manual provides detailed information on how to design a badging template (refer to the Keri CD-ROM). The information provided in this section only provides a brief summary of the design process.

1. If you already have a blank template open, skip to Step 4. Otherwise, double-click the 

icon (on the Windows desktop) to open the GuardDraw program. The GuardDraw main window appears (see Figure 9-2 on page 7 of this section).
2. Click the File ⇒ New pull-down menu.
3. A blank GuardDraw template is now open (see Figure 9-10).

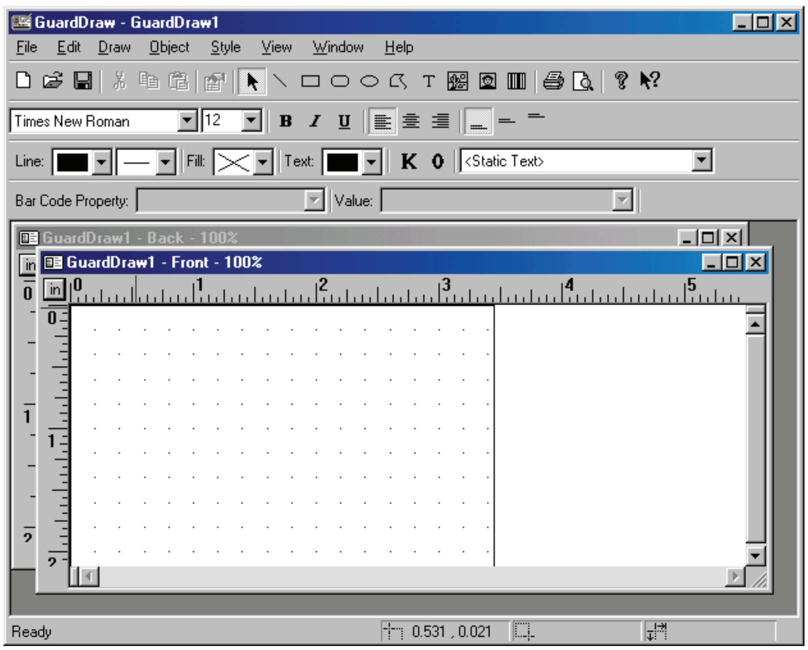


Figure 9-10: A Blank Badge Template Window

4. Verify the correct printer has been selected. If not, “Configuring the Badging Printer” on page 8 of this section for instructions on selecting and configuring the badging printer, and then exit and restart the GuardDraw program.

*NOTE: Prior to opening the GuardDraw program, the badging printer **must** be set as the system default printer. This ensures the correct card/printer margins are applied when the GuardDraw program is opened.*

5. After you have selected your printer, click on File ⇒ Page Setup. The Page Setup window appears (see Figure 9-11 on page 13 of this section).

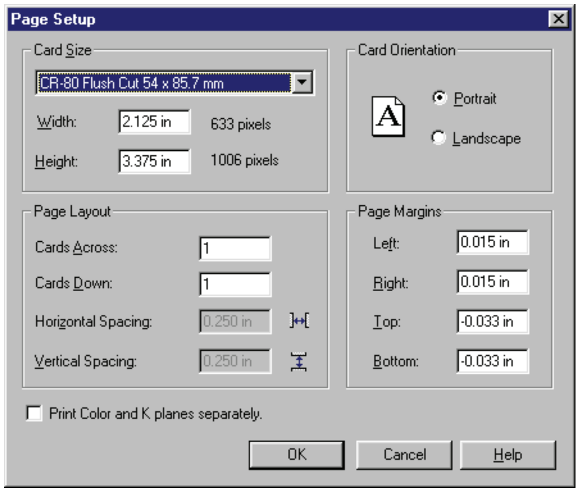


Figure 9-11: Page Setup for a Badge

6. Click the arrow at the right side of the "Card Size" field and a list of available standard card formats appears.
7. Scroll through the list and click the card size format that matches the cards you wish to print.

NOTE: Default values appear in the "Page Margin" fields depending on your selection in the "Card Size" field. Keri Systems recommends using the default page margin values to ensure full coverage of the cards without printing off the card edges.

8. The default values for the "Page Layout" field are set for printing one card as if it is one page in size. This is the correct value for virtually all card printers. If you are printing to a letter sized sheet of paper on a standard ink-jet or laser printer, you can print multiple copies of the same card by adjusting the Cards Across and Cards Down values. The Horizontal and Vertical Spacing values adjust how close together the cards are printed. Because of the differences in card formats and orientation, it may take several tries to correctly determine how many cards, horizontally by vertically, fit on a sheet of paper.
9. In the "Card Orientation" field, click on either the Portrait or Landscape radio button according to the orientation by which the badge will be printed.

NOTE: Your choice between Portrait or Landscape orientation ***must*** *match what you select under printer setup (see Figure 9-8 on page 10 of this section).*

10. Certain badge printers require that the color images be printed separately from the black images. Refer to your badge printer manual and if this is true for your badge printer, click the "Print Color and K planes separately" check box. A check in the box indicates this feature is enabled.
11. Once all badge printing parameters are set, click the OK button. The print parameters are saved and you are ready to create your badge template by following the instructions in your GuardDraw manual.

NOTE: If you are using cards with slot punches, please be aware of the card dimensions for the slot punches when designing your card template.

3.5 Saving the Template

Once the template is complete, it must be placed in the C:\Kerisys\Doors32vX.X\db\badge folder[1] to ensure the *Doors* program can locate and use the template to print a badge.

1. Click the File ⇒ Save pull-down menu. The Save As window appears (see Figure 9-12).



Figure 9-12: The Save As Window

2. Click the at the right side of the “Save in” field and the current folder structure is displayed (see Figure 9-13).

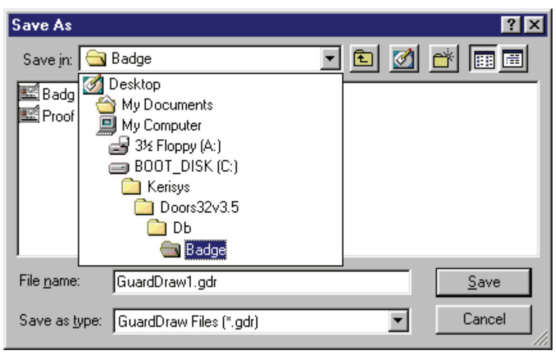


Figure 9-13: The Template Folder Structure

3. Verify the folder path listed in the folder structure[2] is: C:\Kerisys\Doors32vX.X\db\badge\[1].

Doors is now ready for badging operations.

NOTE: Once you have saved a completed template, you may want to save a second copy under a new name for card proofing purposes. Select your default Windows printer for this proofing copy. This will enable you to print examples of the badges from your Doors software to your local printer before you print a badge. However, you must use the template that was originally saved with the badge printer selected when you are ready to print badges.

---

1. X.X is the revision number of the installed *Doors* software.
2. This is automatically set to the default *Doors* installation folder. If you have installed the *Doors* program in a different folder, navigate through the folder structure to locate the *Doors* folder in which you have installed the program.

4.0 Enable Badging in Doors

The enable badging parameter in the System Options allows an operator to enable the photo badge management feature of the *Doors* program. Perform the following steps to enable the Photo ID Badging feature.

1. Click the Setup ⇒ System pull-down menu or click the  button on the tool bar. The Setup System window appears (see Figure 9-14).

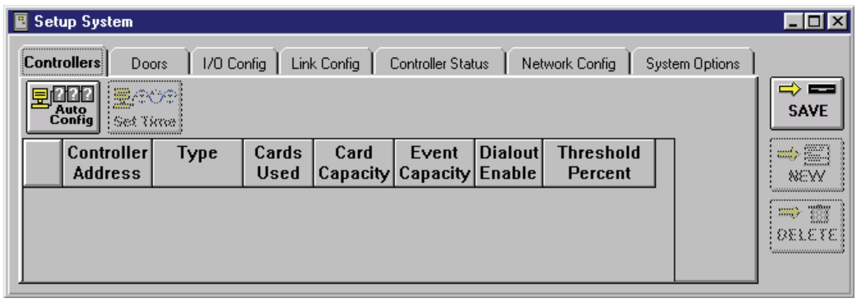


Figure 9-14: Setup System Window

2. Click the **System Options** tab. The System Options window appears (see Figure 9-15).

3. Click the  button to bring up the badging field (see Figure 9-15).

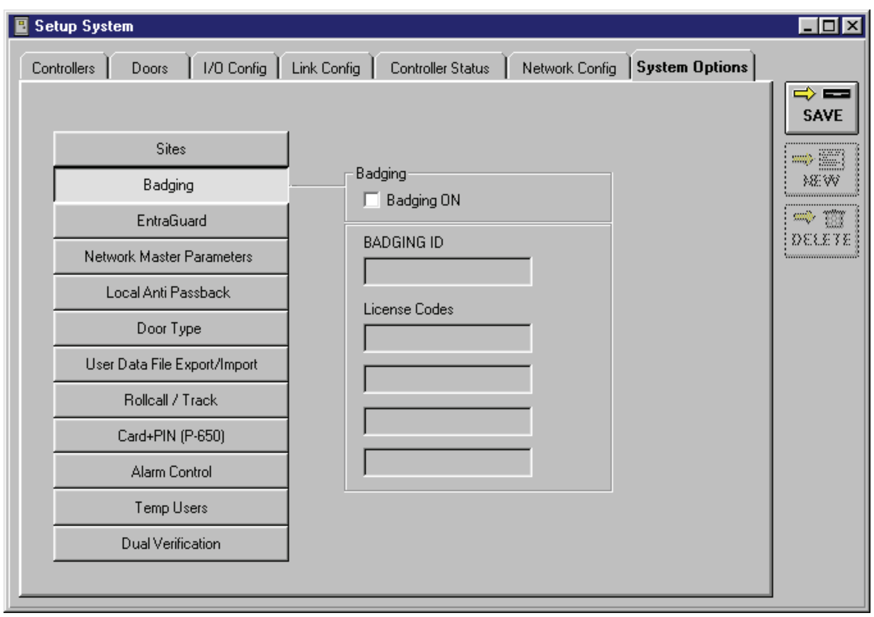


Figure 9-15: System Options Tab – Badging Disabled

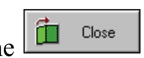
4. If your application does not use badging, verify there is **not** a check mark in the Badging ON box inside the "Badging" field (see Figure 9-15 – this is the default value).

NOTE: You may print sample badges. Sample badges have the word "SAMPLE" watermarked across the face of the badge. To print a badges without the word "SAMPLE" you must have a License Code. To receive a License Code you must call Keri Systems Customer Support at 1-800-260-5265 or 408-451-2520. They will need the PC ID number reported by the Doors program (explained beginning with Step 8 on page 16). With the PC ID number, Customer Support will give you a corresponding License Code. The License Code is assigned to the specific computer used for badging. Badging cannot be moved from one computer to another. If you attempt to do so, the License Code will be invalid and the "SAMPLE" watermark will be printed on cards.

5. To enable badge printing, click in the check box beside the Badging ON option. A check mark appears in the box. When there is a check in the box, the feature is enabled. When the feature is enabled, the Badges Option Changed window appears (see Figure 9-16), verifying you want to make this change.



Figure 9-16: Badges Options Changed Confirmation

6. If you do not want to enable badging at this time, click on the  button. Then click on the  button to save the database without badging enabled.

7. If you choose to enable badging at this time, click on the  button. A Badging Demonstration Acknowledgement window appears (see Figure 9-17) informing you that a license code is necessary to print badges without the "SAMPLE" watermark. Click on the  button. The badging features are all enabled in demo mode.

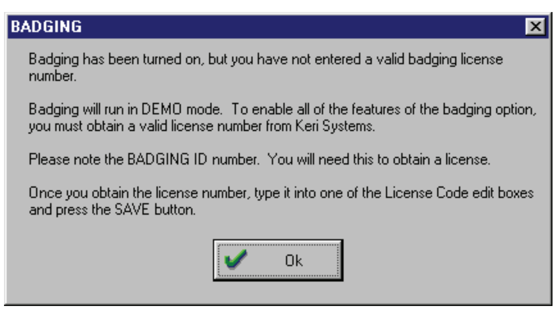


Figure 9-17Badging Demonstration Acknowledgment

8. The Badging ID number should now be visible inside the Badging ID box (see Figure 9-18). Have this number ready when you contact Keri Systems Customer Support to receive your License Code.

9. If you exit without entering a valid License Code, click  then skip to Step 12 on page 17.
10. Enter the License Code received from Keri Systems in the "License Code" field (see Figure 9-18 on page 17 of this section).

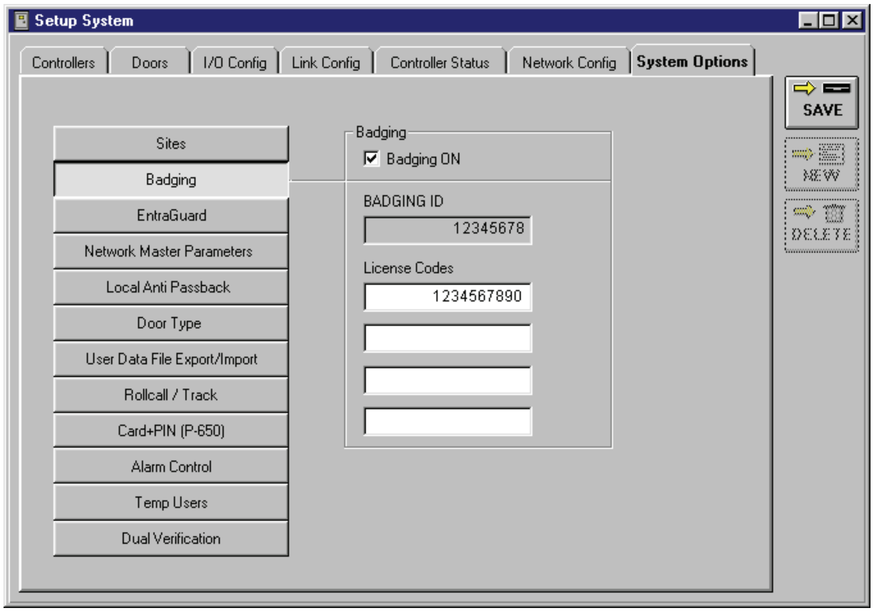


Figure 9-18: System Options Tab – Badging Enabled

11. Once you have entered the License Code, click on the 

button.
12. If you have entered an incorrect License Code, the Badging Demonstration Acknowledgement window appears (see Figure 9-17 on page 16 of this section). Click on the 

button.

NOTE: If you believe this message appeared in error, re-enter the License Code and click on the 

button. If the Demonstration Acknowledgment window reappears, contact Keri Systems Customer Support.

13. A number of database changes are now made to the databases within the *Doors* program to support the badging features. When these changes are complete, the *Doors* program adds two new buttons, 

and 

, to the System ⇒ Setup ⇒ Users spreadsheet to support badge management. If a valid License Code was entered, you are now ready to create and print a badge. If a valid License Code was not entered, all badges will be printed with the word "SAMPLE" watermarked across the face of the card.

NOTE: If the Setup Users window is open, the new buttons will not appear until after you have closed, then re-opened, the Setup Users spreadsheet window.

5.0 Creating and Printing a Badge

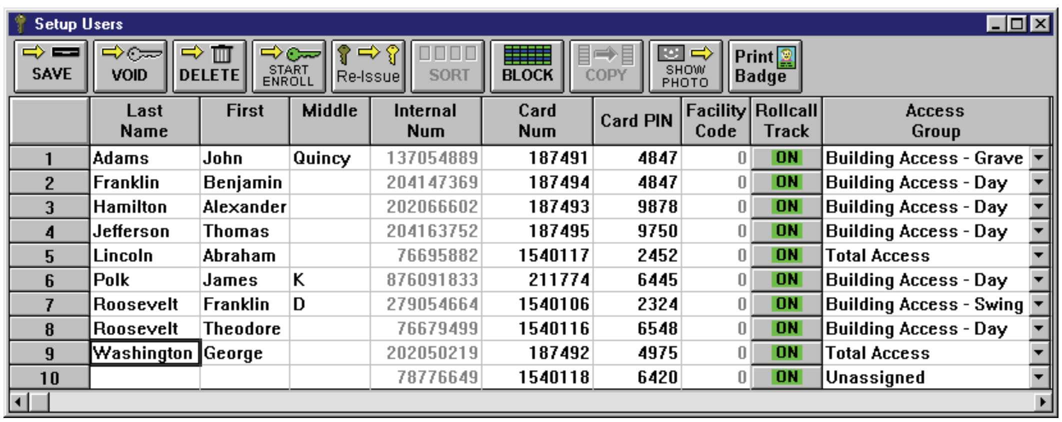
The following instructions describe how to produce and print a badge for a user.

These instructions assume that the card has already been enrolled, the user data has already been entered (including any personal information that may be entered into the personal data fields), the card is turned ON (see "Card Enrollment" on page 3 in section 4), and a card template has been designed in the GuardDraw program (see "Card Template Design" on page 12 of this section).

NOTE: While you are in the badge creation and printing process, the Doors program is unable to perform any other actions (i.e. online monitoring, uploading or downloading information, audible annunciation of events), however the controllers are unaffected and continue normal operation.

5.1 Viewing Badge Information

1. Click the Setup ⇒ Users pull-down menu or click the  button on the tool bar. The Setup Users spreadsheet window appears (see Figure 9-19).



	Last Name	First	Middle	Internal Num	Card Num	Card PIN	Facility Code	Rollcall Track	Access Group
1	Adams	John	Quincy	137054889	187491	4847	0	ON	Building Access - Grave
2	Franklin	Benjamin		204147369	187494	4847	0	ON	Building Access - Day
3	Hamilton	Alexander		202066602	187493	9878	0	ON	Building Access - Day
4	Jefferson	Thomas		204163752	187495	9750	0	ON	Building Access - Day
5	Lincoln	Abraham		76695882	1540117	2452	0	ON	Total Access
6	Polk	James	K	876091833	211774	6445	0	ON	Building Access - Day
7	Roosevelt	Franklin	D	279054664	1540106	2324	0	ON	Building Access - Swing
8	Roosevelt	Theodore		76679499	1540116	6548	0	ON	Building Access - Day
9	Washington	George		202050219	187492	4975	0	ON	Total Access
10				78776649	1540118	6420	0	ON	Unassigned

Figure 9-19: Setup Users Window

2. Click the name of the user to whom a badge is to be issued (see Figure 9-19).

3. Click on the  button and the View Badge Information window appears (see Figure 9-20 on page 19 of this section).

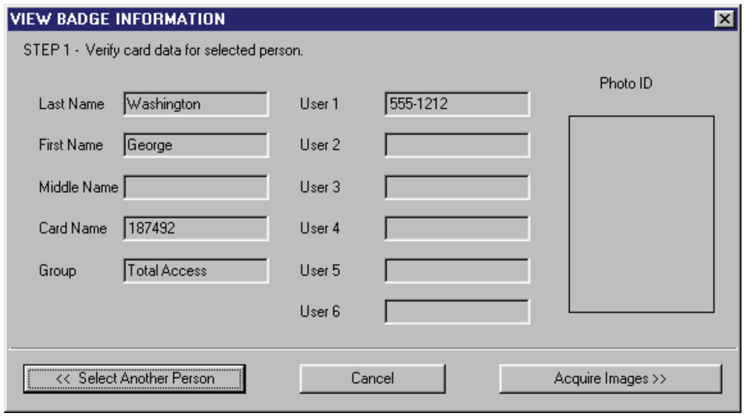
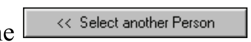


Figure 9-20: View Badge Information

4. The Badging Wizard automatically imports and displays available information from the user database into the data fields in the badging wizard.
5. To exit the Badging Wizard, click on the 

button.
6. If an incorrect user has been selected, click on the 

button and return to Step 2 on page 18.
7. To acquire or edit user photos, click on the 

button.

5.2 Acquire and Edit User Photo

1. Continuing from Step 7 and Figure 9-20 above, click on the Acquire Images >> button. The Acquire and Edit Images window appears (see Figure 9-21).

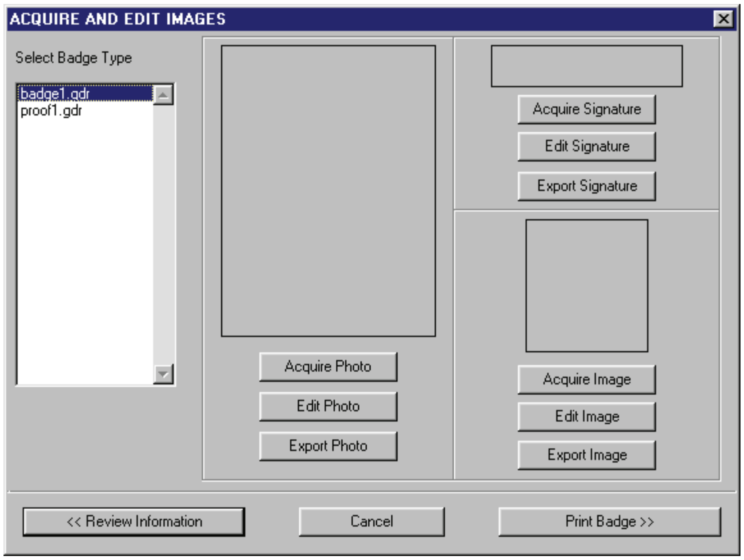


Figure 9-21: Acquire and Edit Images

2. In the Select Badge Type field, click on the badge template you want to use for this user (Figure 9-21). If the Select Badge Type field is empty, you need to create a badge template in the GuardDraw program (see “Badge Templates” on page 6 of this section).

NOTE: If you are making a proof of a card to be checked for accuracy before printing a badge, select the Badge Type you have previously set up for your default Windows printer. If you are ready to print a badge, be sure you select the Badge Type set up for your badge printer.

3. To acquire a photograph for this user, click on the Acquire Photo button. The Select Photo Source window appears (see Figure 9-22).

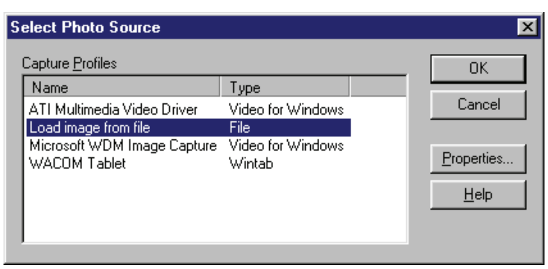


Figure 9-22: Select Photo Source

4. Scroll through the list of available sources, select the source for your user photograph, and click on the OK button. Depending upon the source of the photograph, different steps may be required to create or locate the photograph.

NOTE: Because of the variety of possible sources for photographs, specific information for creating the photograph cannot be given here. Please refer to the documentation for that source device on how to create the photograph.

5. Once the photograph has been created/located, the photograph is placed into the Image Enhancement window where it can be edited to improve the quality of the image as it will be printed on the badge (see Figure 9-23).

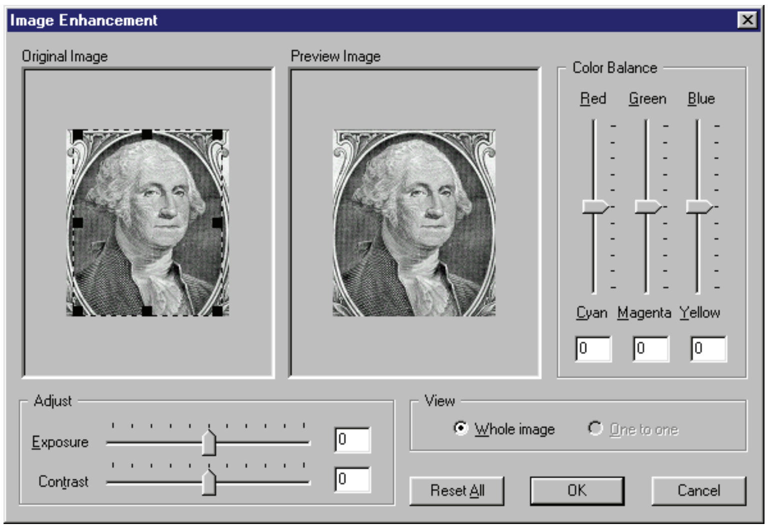


Figure 9-23: Image Enhancement

6. A variety of adjustments can be made to improve the quality of the photograph. At all times, a copy of the original photograph is kept in the Original Image pane of the Image Enhancement window. All adjustments are made to the photograph in the Preview Image pane of the Image Enhancement window. The following adjustments can be made.

   - Exposure – to brighten or darken the image.
   - Contrast – to emphasize or de-emphasize the difference between light and dark portions of the image.
   - Red/Cyan Color Balance – to adjust the amount of Red/Cyan tint in the image.
   - Green/Magenta Color Balance – to adjust the amount of Green/Magenta tint in the image.
   - Blue/Yellow Color Balance – to adjust the amount of Blue/Yellow tint in the image.

   Make these adjustments as necessary to improve the quality of the photograph image. If you become dissatisfied with all the adjustments made, you can always return to the original image by clicking on the Reset All button.

   To view the entire photograph image, click on the **Whole Image** radio button. The entire image is resized and displayed in both the Original and Preview image panes. To view the photograph image in the perspective in which it will be printed, click on the **One to One** radio button. The image is displayed in both the Original and Preview image panes in its original size, which may be either smaller or larger than the pane size.

7. To exit the Image Enhancement window without making any changes, click on the Cancel button. You can either start the Acquire Photo process all over again (return to Step 1 on page 20) or exit the Badging Wizard entirely by clicking on the Cancel button again.

8. If you are satisfied with your adjustments, click on the 

button. The Acquire and Edit Images window appears with the user photo displayed (see Figure 9-24).

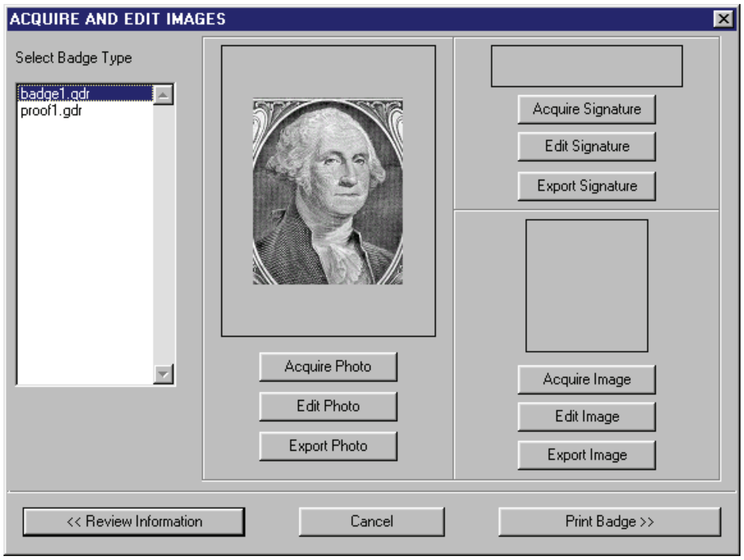


Figure 9-24Acquire and Edit Images Window with User Photo

9. If desired, the user image can be exported to one of a variety of graphic file formats. Click on the 

button. A file Save As window appears (see Figure 9-25).

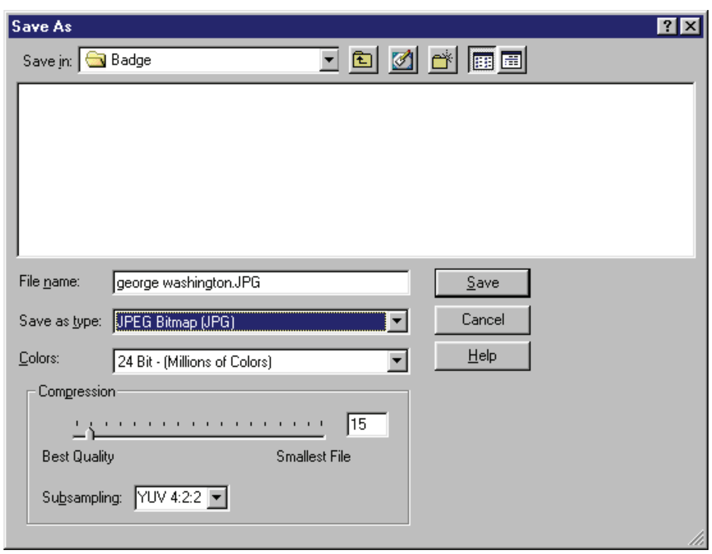


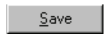
Figure 9-25Export User Photo

10. Click the “File name” field and enter a descriptive file name.

11. Click the  at the right side of the “Save as type” field. A list of available graphic export photo types appears. Scroll through the list and select the desired file type.

12. Click the  at the right side of the “Colors” field. A list of available color resolution values appears. Scroll through the list and select the desired color resolution.

NOTE: The greater the number of colors, the better the image, but the larger the file size will be. The settings in the "Compression" field are automatically set at standard values for the file type selected. Unless you are familiar with graphic file compression, it is recommended that you leave the Compression settings at their standard values.

13. By default, the exported user photo file is saved in the same folder with the original user photo. If the photo file should be saved in a different folder, click the  at the right side of the "Save in" field. Navigate through the folders in the host computer's hard disk drive until you locate the desired folder. Click on the 

button. The user photo file is exported and the Acquire and Edit Images window reappears (see Figure 9-24 on page 22 of this section).
14. Once the user photo has been acquired, you have three options.

    - To acquire a secondary image, skip to "Acquire and Edit Images" below.
    - To acquire a digital signature, skip to "Acquire and Edit Signatures" on page 24 of this section.
    - If you are ready to print a card, click the 

button and skip to "Preview and Print a Badge" on page 29 of this section.

5.3 Acquire and Edit Images

An image can be acquired to provide an extra level of security. Any type of graphic image can be used; such as a fingerprint or an alternate photograph of the user. The process for acquiring and editing an image is exactly the same as that for acquiring and editing a user photo. Follow the instructions in "Acquire and Edit User Photo" on page 20 of this section, replacing the Photo buttons with the corresponding Image buttons.

5.4 Acquire and Edit Signatures

User signature images can be acquired either by using a digital tablet or by scanning an image of a user's signature.

The following instructions describe the process for acquiring and editing a signature from a digital signature pad, starting from the Acquire and Edit Images window with a user photo (see Figure 9-26).

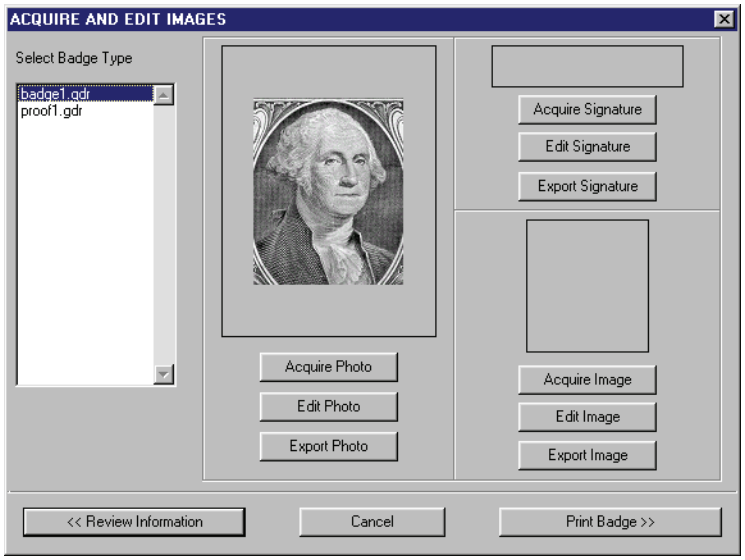


Figure 9-26: Acquire and Edit Images

1. To acquire a digital signature for this user, click on the Acquire Signature button. The Select Signature Source window appears (see Figure 9-27).

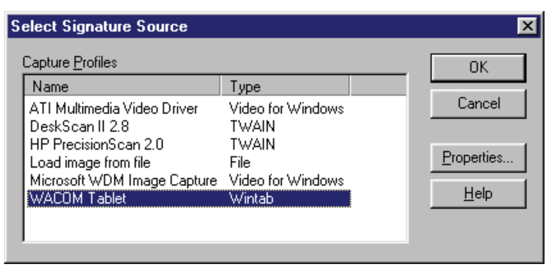


Figure 9-27: Select Signature Source

2. Scroll through the list of available sources and select the source for the digital tablet. The first time a digital tablet is used to input a signature, the tablet's operating parameters must be set. Once set, the parameters are remembered and do not need to be entered again. If the tablet operating parameters are already set, skip to Step 7 on page 26.
3. To set the digital tablet's operating parameters, click on the Properties... button. The Capture Profile Properties window appears, displaying the Image Enhancements tab (see Figure 9-28 on page 25 of this section).

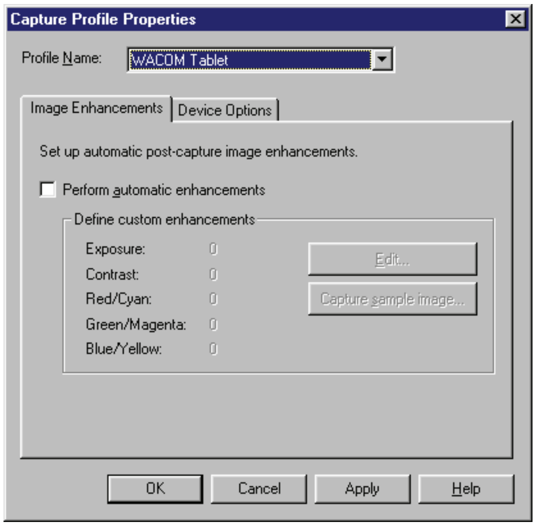


Figure 9-28: Capture Profile Properties

4. The Perform Automatic Enhancements check box should be blank, allowing you the flexibility to edit a signature image if necessary. Click on the Device Options tab. The Device Options tab appears (see Figure 9-29).

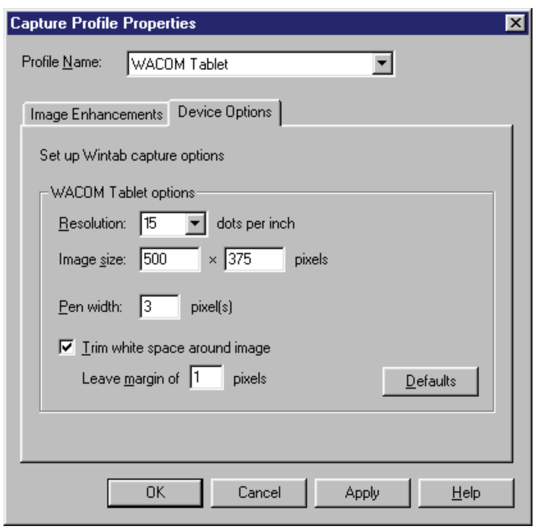


Figure 9-29: Device Options Tab

5. To ensure the proper aspect ratio for digital signatures, the tablet options must be set as displayed in Figure 9-29.
   - Image Size has two fields: width x height. Click the width field and enter 500. The height field will automatically be set with the matching aspect ratio value.
   - Click the “Resolution” field and set the resolution to 15.
   - Click the “Pen Width” field and set the pen width to 3. This value may need to be adjusted depending upon how hard the users press down on the digital pad when entering their signatures.
   - Verify there is a check mark in the Trim White Space Around Image check box, click in the “Leave Margin” field and set the value to 1.

6. Once all these values are set, click on the Apply button followed by the OK button. The Select Signature Source window re-appears (see Figure 9-27 on page 24 of this section).
7. Click on the OK button and the Capture Signature window appears (see Figure 9-30).

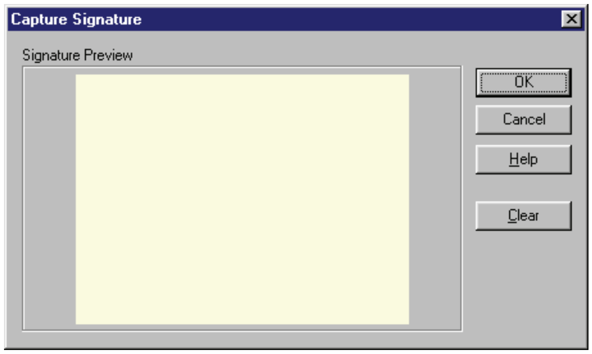


Figure 9-30Capture Signature Window

8. Have the user take the stylus in hand and enter a signature, just like signing a piece of paper. As the signature is written, it appears in the Capture Signature window (see Figure 9-31).

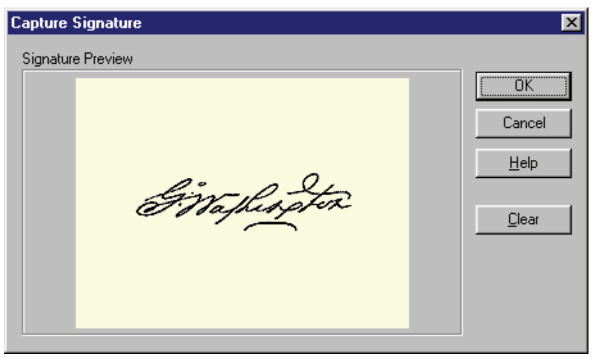


Figure 9-31Capture Signature Window with Signature

9. If the quality of the signature is not acceptable, click on the Clear button. The Capture Signature window is cleared and ready to accept another signature. Repeat Step 8.
10. When an acceptable signature is entered, click on the OK button. The Image Enhancement window appears (see Figure 9-32 on page 27 of this section).

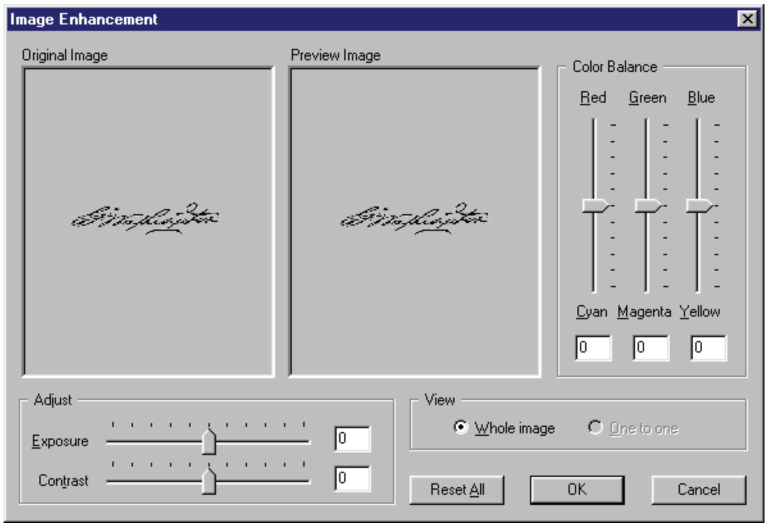


Figure 9-32Signature Image Enhancement

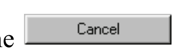
11. A variety of adjustments can be made to improve the quality of the signature. At all times, a copy of the original signature is kept in the Original Image pane of the Image Enhancement window. All adjustments are made to the photograph in the Preview Image pane of the Image Enhancement window. The following adjustments can be made.

    - Exposure – to brighten or darken the image.
    - Contrast – to emphasize or de-emphasize the difference between light and dark portions of the image.
    - Red/Cyan Color Balance – to adjust the amount of Red/Cyan tint in the image.
    - Green/Magenta Color Balance – to adjust the amount of Green/Magenta tint in the image.
    - Blue/Yellow Color Balance – to adjust the amount of Blue/Yellow tint in the image.

    Make these adjustments as necessary to improve the quality of the signature image. If you become dissatisfied with all the adjustments made, you can always return to the original image by clicking on the 

 button.

    To view the entire signature image, click on the **Whole Image** radio button. The entire image is resized and displayed in both the Original and Preview image panes. To view the signature image in the perspective in which it will be printed, click on the **One to One** radio button. The image is displayed in both the Original and Preview image panes in its original size, which may be either smaller or larger than the pane size.

12. To exit the Image Enhancement window without making any changes, click on the 

 button. You can either start the Acquire Signature process all over again (return to Step 1 on page 24) or exit the Badging Wizard entirely by clicking the 

 button again.
13. If you are satisfied with your adjustments, click on the 

 button. The Acquire and Edit Images window appears with the user photo displayed (see Figure 9-33 on page 28 of this section).

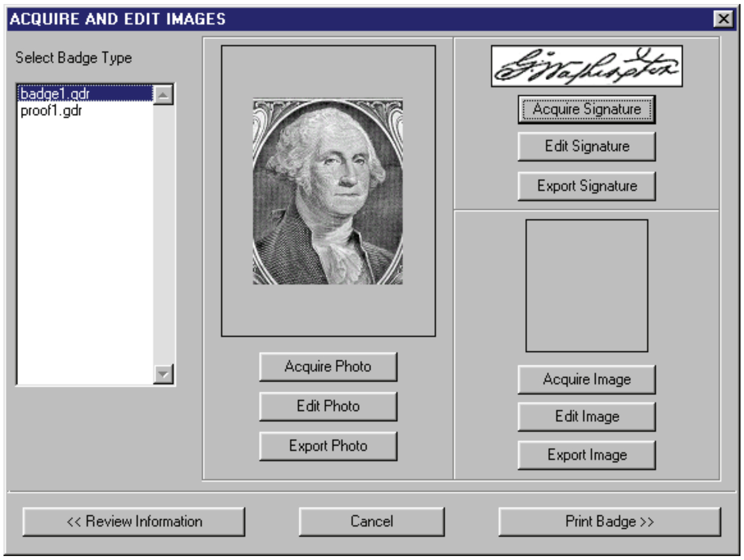


Figure 9-33Acquire and Edit Images Window with Photo and Signature

14. If desired, the signature image can be exported to one of a variety of graphic file formats. Click the 

button. A file Save As window appears (see Figure 9-34).

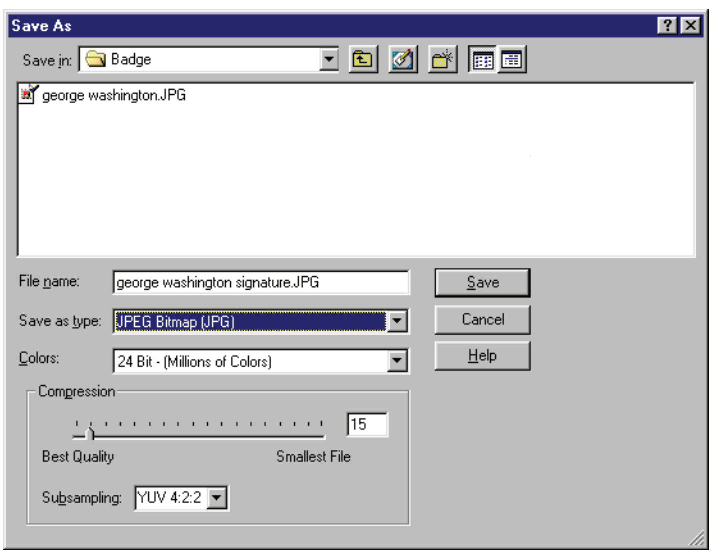


Figure 9-34Export User Signature

15. Click the “File name” field and enter a descriptive file name.
16. Click the  at the right side of the “Save as type” field. A list of available graphic export photo types appears. Scroll through the list and select the desired file type.
17. Click the  at the right side of the “Colors” field. A list of available color resolution values appears. Scroll through the list and select the desired color resolution.

NOTE: The greater the number of colors, the better the image, but the larger the file size will be. The settings in the "Compression" field are automatically set at standard values for the file type selected. Unless you are familiar with graphic file compression, it is recommended that you leave the Compression settings at their standard values.

18. By default, the exported user signature file is saved in the same folder with the original user photo. If the signature file should be saved in a different folder, click the at the right side of the "Save in" field. Navigate through the folders in the host computer's hard disk drive until you locate the desired folder. Click on the Save button. The user signature file is exported and the Acquire and Edit Images window reappears (see Figure 9-33 on page 28 of this section).
19. Once the user signature has been acquired, you have three options.

    - To acquire a user photo, skip to "Acquire and Edit User Photo" on page 20 of this section.
    - To acquire a secondary image, skip to "Acquire and Edit Images" on page 23 of this section.
    - If you are ready to print a card, click on the Print Badge >> button and skip to "Preview and Print a Badge" below.

5.5 Preview and Print a Badge

Once all information and images applicable to the user are collected, the badge is ready to print.

1. Click on the Print Badge >> button and the Preview and Print Badge window opens and a sample of the badge is displayed (see Figure 9-35).

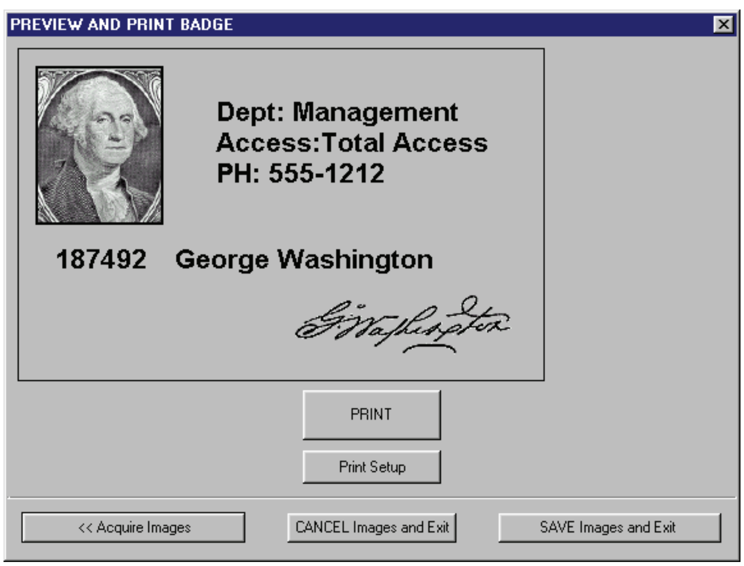


Figure 9-35Preview and Print a Single-Sided Badge

2. If the badge is two-sided, the window adjusts its size to display both sides of the badge (see Figure 9-36 on page 30 of this section).

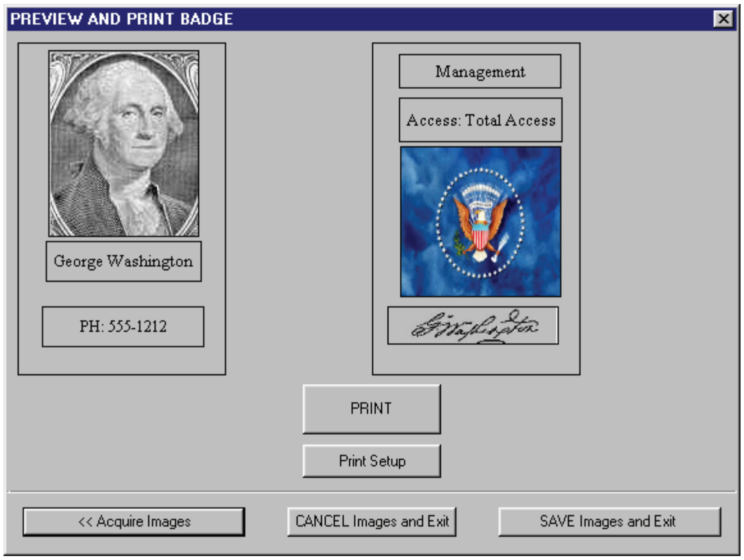


Figure 9-36Preview and Print a Double-Sided Badge

3. To cancel the entire Badging process, click on the [CANCEL Images and Exit] button.
4. To return to the Acquire and Edit Photos window (to make a change to the user photo, signature, or image files), click on the [<< Acquire Images] button.
5. To save the user photo, signature, or image files without printing a badge, click on the [SAVE Images and Exit] button.
6. When you are ready to print the badge, click on the [PRINT] button. After a several second delay, the badge is printed. If you are printing a double-sided badge on a single-sided printer, the first side will be automatically sent to the printer and the Two-Side Print Badge Window will appear (see Figure 9-37).

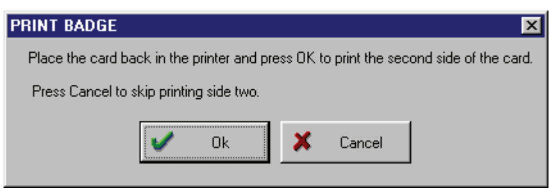


Figure 9-37Two-Side Print Badge Window

7. Once the first side has been printed and you have flipped the badge over, click on the [OK] button to print the second side.
8. Click on the [SAVE Images and Exit] button and the Preview and Print Badge window closes.

6.0 Show Photo

The following instructions explain how to show a user photo image from the *Doors* program. For display of a user photo while monitoring, see “Display Photo While Monitoring” on page 42 in section 5.

1. In the Setup Users spreadsheet window, click on a cell for the user for which the photo image should be shown (see Figure 9-38).

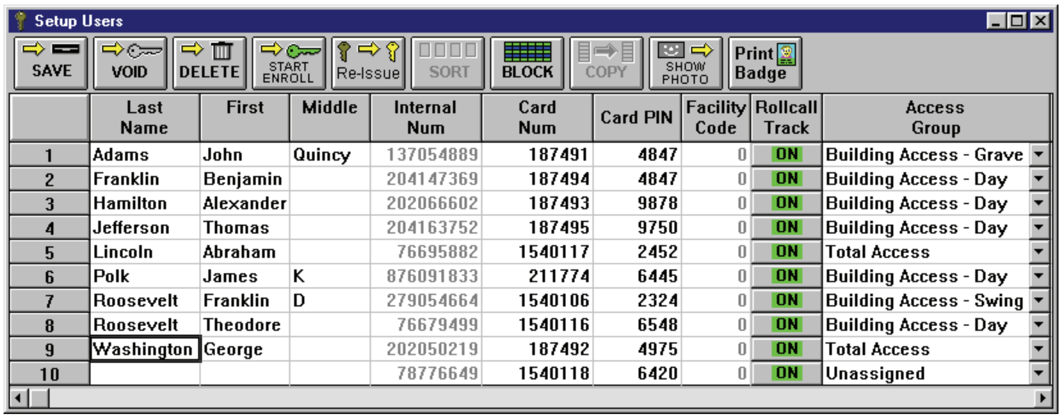


Figure 9-38: Setup Users Window

2. Click on the 

button.
3. If a photo image file exists for the selected user, the photo is shown in the Photo window (see Figure 9-39).

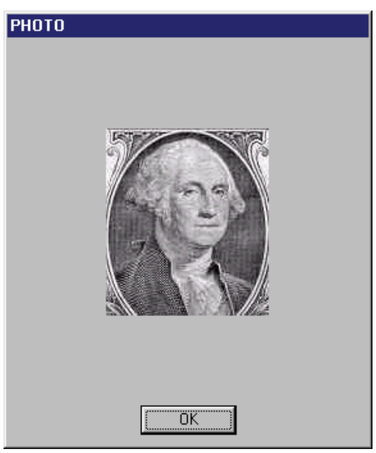


Figure 9-39: Show User Photo Image File

4. If there is no photo image file for the selected user a “Photo Not Found” window appears (see Figure 9-40 on page 32 of this section).



Figure 9-40: Photo Not Found

5. Click on the  button and either select another user or return to "Acquire and Edit User Photo" on page 20 of this section to associate a photo image with this use.

Section 10

EntraGuard

The EntraGuard Telephone Entry Controller contains all the intelligence and necessary inputs/outputs to manage access through one door. Users (tenants) may gain or grant access through one of two ways:

- entering an assigned User ID at the EntraGuard unit
- granting access from dwelling by pressing a designated number on any regular phone within the dwelling

The EntraGuard unit may be used by itself or connect to a PXL network. When connected to a PXL network, the EntraGuard unit acts as any other PXL access control unit on a network.

The EntraGuard controller is managed through the *Doors* program; via modem, TCP/IP, or direct connect. When the EntraGuard feature is enabled, a number of windows throughout the *Doors* program are modified and the supporting databases are changed, adding the necessary hooks to support an EntraGuard unit.

This section describes the necessary steps to setting up an EntraGuard unit.

- The process for enabling the EntraGuard feature.
- The process for configuring EntraGuard parameters.
- The process for enrolling EntraGuard User IDs.
- The differences in database entry and program operation.

Document Number 01914-010, Revision 5.4 – April, 2006

1.0 Enable EntraGuard

If you have an EntraGuard controller connected to the access control system, the feature needs to be enabled in *Doors.*

NOTE: The EntraGuard feature is automatically enabled if an EntraGuard unit is detected when an autoconfiguration is performed on the system.

1. To manually enable the EntraGuard feature, click on the Setup ⇒ System pull-down menu or click on the  button on the tool bar, then click on the **System Options** tab. The System Options window appears.
2. Click on the 

button. The System Options window will reveal the EntraGuard field where EntraGuard options may be set (see Figure 10-1).

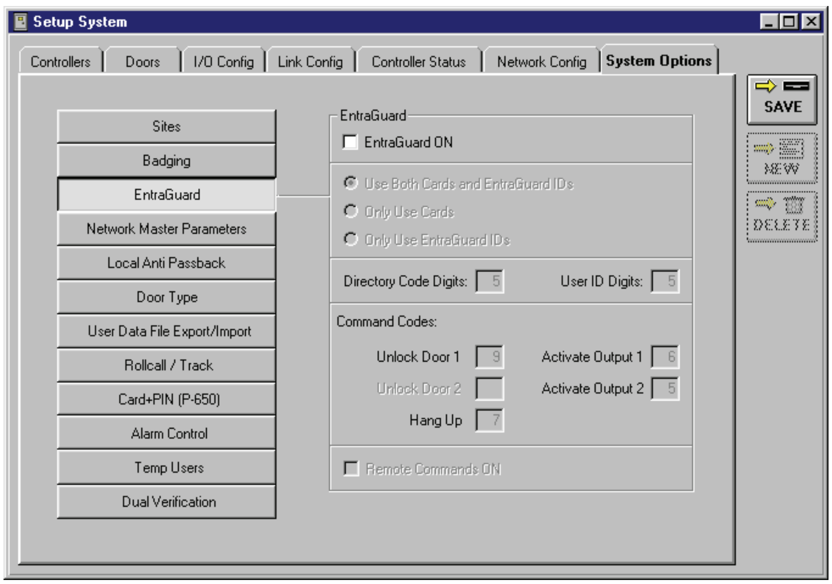


Figure 10-1: System Options Tab - EntraGuard Disabled

3. Click on the **EntraGuard ON** check box. A check mark appears in the box. Because the changes required to implement the EntraGuard feature make major changes to the *Doors* program and its supporting databases, a confirmation window appears (see Figure 10-2).

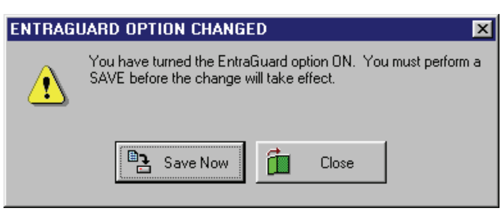
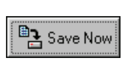


Figure 10-2: EntraGuard Option Changed - ON

4. Click on the 

button and the conversion to EntraGuard mode automatically occurs.
5. The EntraGuard fields change from grey to black letting you know it is available for editing of specific EntraGuard options (see Figure 10-3 on page 4 of this section).

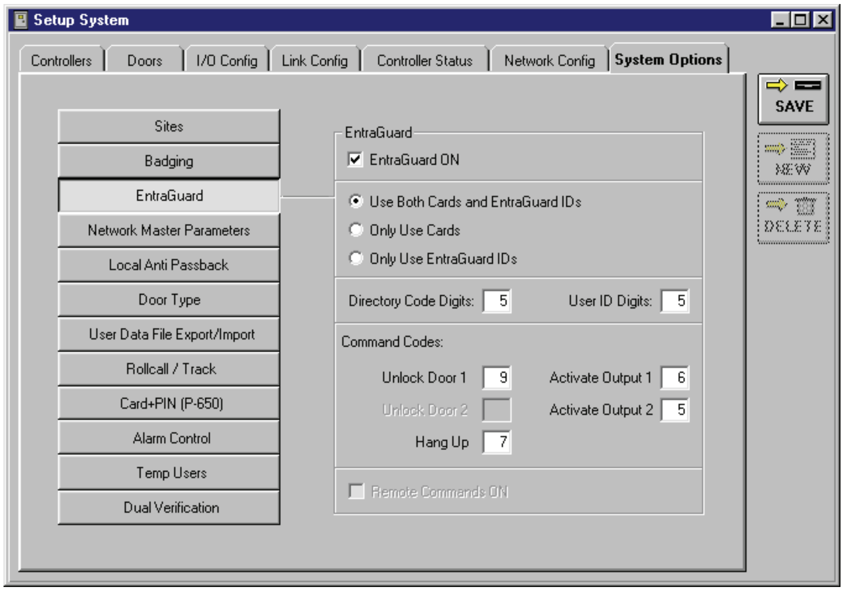


Figure 10-3: System Options Tab - EntraGuard Enabled

1.1 Select Enrollment Options

You must select the type of system the EntraGuard controller is connected to. Your selection in the second field will affect the enrollment options you will have further in the setup process.

- Use Both Cards and EntraGuard IDs - Selecting this option will allow for both enrollment of cards and User IDs in any combination. This is the default value.
- Only Use Cards - Selecting this option will limit enrollment to cards only (including the Card+PIN option). If any users will need a User ID assigned to them, do not choose this option.
- Only Use EntraGuard IDs - Selecting this option will limit enrollment to User IDs only. If any users will need a card assigned to them, do not choose this option.

1.2 Select Directory Code and User ID Digits

Directory Code Digits

The number shown in the Directory Code Digits box determines the number of digits in the code listed in the EntraGuard directory. The directory code is the set of numbers used by visitors at the EntraGuard controller to dial up the person they wish to contact. The tenant may then either grant or deny visitor access to the building. The default for this field is 5.

User ID Digits

The number shown in the User ID Digits box determines the number of digits in the User ID assigned to each user. A user enters their User ID to gain access through an EntraGuard controlled door. The default for this field is 5.

NOTE: Great care should be taken when determining the digits in these fields. Once you have selected directory codes and enrolled User IDs according to the selections you make here, you will not be able to decrease the number of digits used. However, you will be allowed to increase the number of digits for both of these categories. When the number of digits is increased additional zeros are added to the beginning of previously enrolled users. These additional zeros must be used from that point on.

1.3 Command Codes

Command codes are the telephone keys used to perform certain functions such as allow entry through the EntraGuard controlled door, etc. See Figure 10-3 on page 4 of this section for their location in the EntraGuard field.

Unlock Door 1
The number in this field determines the telephone key assigned to allow access through the EntraGuard controlled door. The default for this field is 9.

Unlock Door 2
Although the default for this field is set at 8, this field is not used at this time.

Hang Up
The number in this field determines the telephone key assigned to disconnect from the EntraGuard controller without granting access. The default for this field is 7.

Activate Output 1
The number in this field determines the telephone key assigned to activate output 1. This may be something such as turning on lights, etc. The default for this field is 6.

Activate Output 2
The number in this field determines the telephone key assigned to activate output 2. The default for this field is 5.

NOTE: It is possible to assign the same telephone key to all of these fields, but care should be taken to make sure that all of these functions are needed at the same time.

1. To change the default values for any of these fields, click in the window you want to change. Delete the number that is there and enter the number of your choice.
2. Click on the 

button to save these changes. If the EntraGuard parameters are not saved before clicking any other button or exiting the System Setup window, the data entered is lost and must be re-entered.
3. You must update the access control network with the new information. Click on the 

button on the tool bar (for details on the update process refer to “Update the Network” on page 35 in section 5).

1.4 Remote Commands

The Remote Commands option is for future use. The default is for Remote Commands to be disabled (no check in the Remote Commands ON check box). Leave the box in its default state.

2.0 Setup Dial Time Zones

Once an EntraGuard controller is in use, time zones have an additional use. A Dial Timezone must be applied to the EntraGuard controller defining the hours a tenant will accept a call from visitors requesting access through the EntraGuard unit. The process to set up a Dial Timezone is the same as setting up any time zone (see "Setup Time Zones" on page 3 in section 3).

The difference is in where the time zone is applied.

- A time zone applied to the controller in the Dial Timezone column in the Setup System window defines the daily hours when a tenant will accept calls from visitors using the EntraGuard unit.
- A time zone applied through an access group determines when a user is allowed entry through any controlled door including an EntraGuard controlled door.

3.0 Setup Controllers/Doors

With the addition of an EntraGuard unit to the access control network, certain changes are made to the databases to allow for specific EntraGuard configurations.

3.1 Controller Configuration

Columns are added to the Controller tab once the EntraGuard feature has been enabled. The following is a list of those new columns.

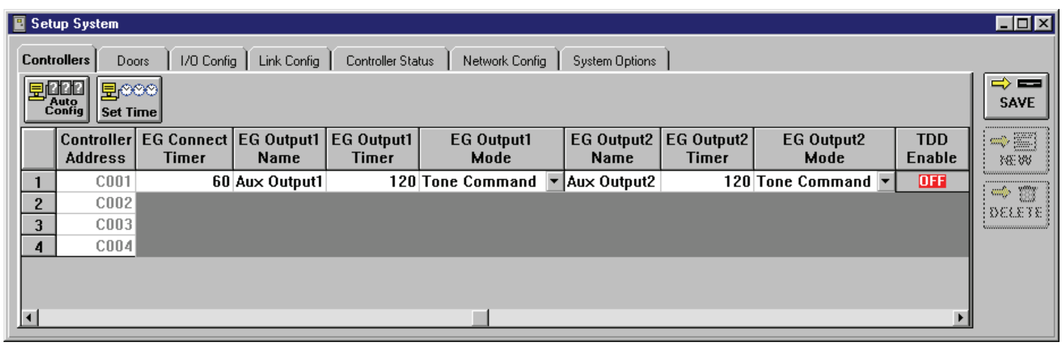


Figure 10-4: Setup System Controllers Tab – Part 1

EG Connect Timer
The EG Connect Timer determines the length of connection between the EntraGuard unit and the tenant's telephone. Once the time set has been reached, the connection will cease. The time shown is in seconds and may be set to anything between 30 - 255 seconds. The default is set to 60 seconds.

EG Output1 & EG Output2
Name – description of what the EG Output controls (i.e. Lobby Lights)
Timer – determines the amount of time in seconds the output is in effect (the default is set to 120)
Mode – determines what actions will activate an output

- Disabled - outputs are not disabled and not activated in any condition
- Tone Command - by a valid telephone command
- Access Granted - when a valid access request is granted
- Both Tone and Access - both a valid telephone command or a granted access request

TDD Enable
Not used at this time. Should remain in the OFF position.

3.1.1 EntraGuard Banner Messages

The EntraGuard LCD (located on the front of the EntraGuard controller) is capable of rotating 3 banner messages. The space available is determined by the EntraGuard controller in use.

3.1.1.1 Edit Gold/Titanium Banner Message

The EntraGuard LCD (located on the front of the EntraGuard Gold/Titanium controller) is capable of rotating 3 banner messages made up of 80 characters each. Spacing is limited so carefully plan what each banner message will say.

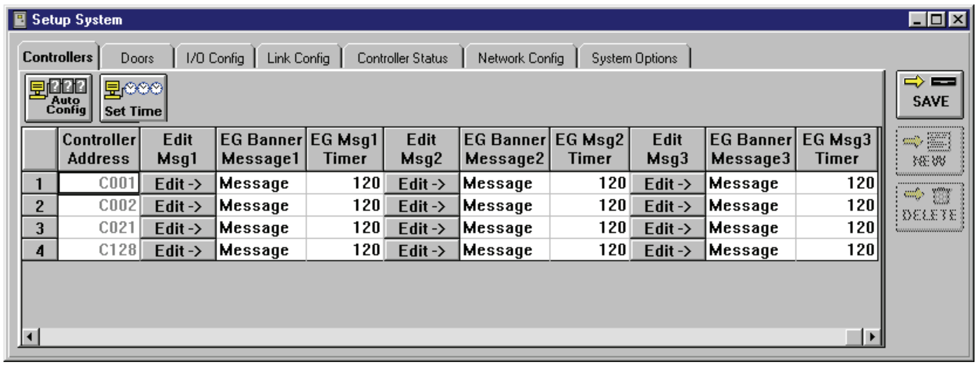


Figure 10-5: Setup System Controllers Tab – Part 2 (EntraGuard Gold/Titanium)

Edit Msg#

Click on the 

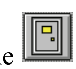
button to bring up the edit message window (see “Edit Gold/Titanium Banner Message” below).

EG Banner Message#

This field shows what is entered as the message banner.

EG Msg Timer#

This field determines the amount of time each message should be shown on the EntraGuard LCD before going on to the next message. For best readability it is recommended this be set for 10 seconds.

1. To edit the banner message, click on the Setup ⇒ System pull-down menu or click on the  tool bar button. Then click on the **Controllers** tab. The Controllers window appears (see Figure 10-5).
2. Scan down the controller addresses column and locate the EntraGuard controller.
3. Scroll across that controller’s row in the spreadsheet and locate the **Edit Msg1** column (see Figure 10-5).
4. Click on the 

button. The Edit Banner Message window will appear (see Figure 10-6).

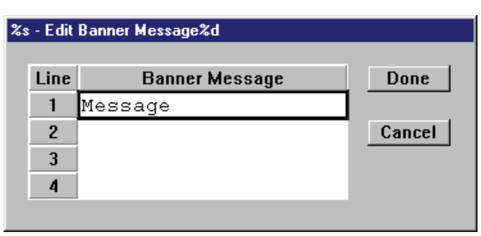


Figure 10-6: Edit Banner Message1 Window

5. Enter the message for banner 1. For example enter:

Line 1: **WELCOME TO THE**
Line 2: **AMERICAN HERITAGE**
Line 3: **VILLA APTS. TO USE**
Line 4: **THE ALPHA DIRECTORY,**

6. The Edit Banner Message window should look similar to Figure 10-7.

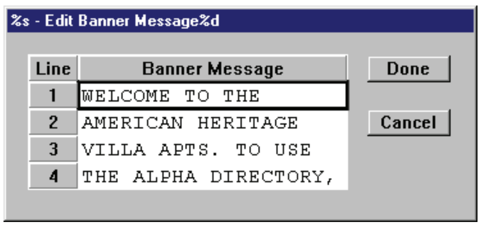


Figure 10-7: Edit Banner Message1 Window Filled

7. Once you are satisfied with the message, click on the Done button. The message will appear in the EG Banner Message1 column (see Figure 10-8).

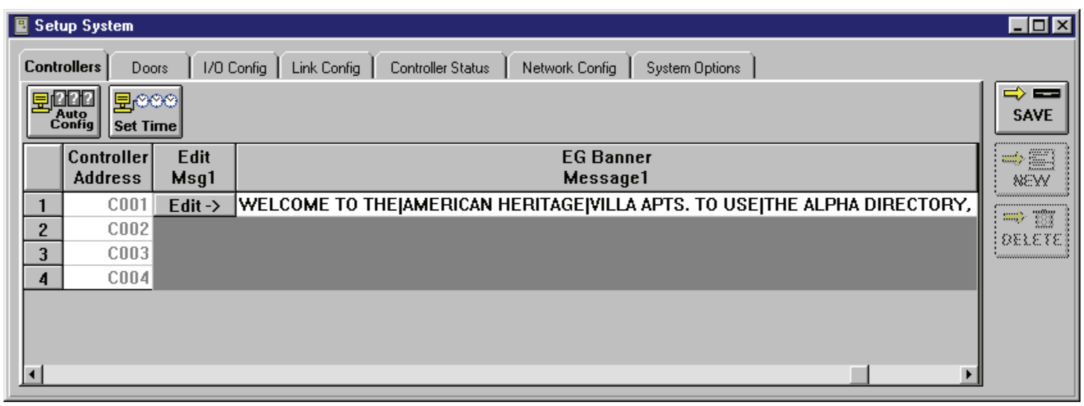


Figure 10-8: Banner Message1 Column

8. Repeat steps 4-7 for messages 2 and 3.

<u>EG Banner Message2 Sample</u>
Line 1: **HIGHLIGHT THE LETTER**
Line 2: **KEYS BY SELECTING**
Line 3: **THE #/A KEY. ENTER**
Line 4: **THE FIRST LETTERS OF**

<u>EG Banner Message3 Sample</u>
Line 1: **THE LAST NAME OF THE**
Line 2: **TENANT. WHEN ARROW**
Line 3: **POINTS AT NAME,**
Line 4: **PRESS CALL.**

9. Click on the 

button to save these changes. If the banner messages are not saved before clicking any other button or exiting the System Setup window, the data entered is lost and must be re-entered.

10. You must update the access control network with the new information. Click on the 

button on the tool bar (for details on the update process refer to “Update the Network” on page 35 in section 5).

3.1.1.2 Edit Platinum Banner Message

The EntraGuard LCD (located on the front of the EntraGuard Platinum controller) is capable of rotating up to 3 banner messages. There are two font sizes that may be selected on the EntraGuard Platinum. Because the user may choose their font size, each banner message must be written in two windows. One for large size fonts and the other for small size fonts (default font). The large size font banner message may contain up to 24 characters per line with 7 lines maximum. The small size font banner message may contain up to 24 characters per line with 10 lines maximum. Spacing is limited so carefully plan what each banner message will say.

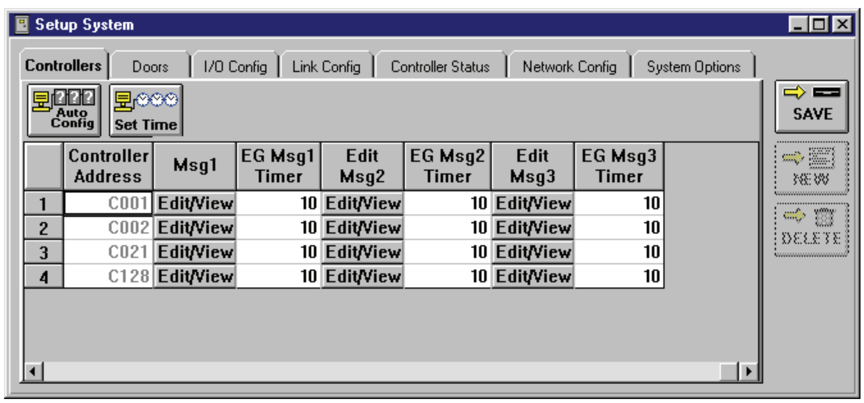


Figure 10-9: Setup System Controllers Tab – Part 2 (EntraGuard Platinum)

Msg# or Edit Msg#

Click on the 

button to bring up the message window.

EG Msg# Timer

This field determines the amount of time each message should be shown on the EntraGuard LCD before going on to the next message. For best readability it is recommended this be set for 10 seconds. To not use one of the banners, set the time for 0 seconds.

1. To edit the banner message, click on the Setup ⇒ System pull-down menu or click on the  tool bar button. Then click on the **Controllers** tab. The Controllers window appears (see Figure 10-9).
2. Scan down the controller addresses column and locate the EntraGuard controller.
3. Scroll across that controller’s row in the spreadsheet and locate the **Msg1** column (see Figure 10-9).
4. Click on the 

button. The “Edit/View Banner Message1 with large font” window will appear (see Figure 10-10 on page 10 of this section).

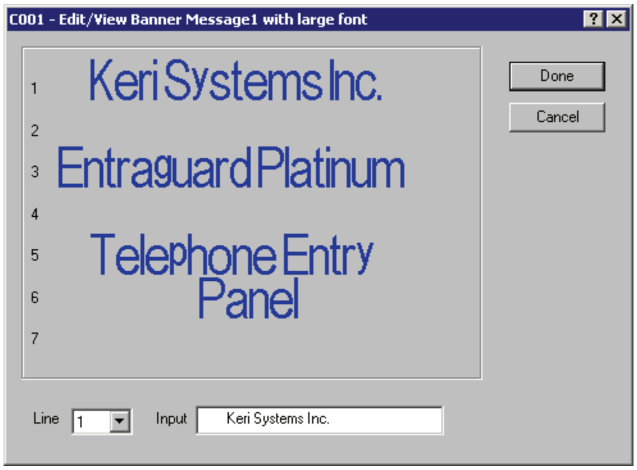


Figure 10-10: Edit/View Platinum Banner Message1 Window - Default

5. The message banner must be edited line by line. The line numbers are shown as a guide on the left of the window.
6. To edit a line, click on the "Line" drop-down menu at the bottom of the screen and select the desired line to edit.
7. Next, click in the "Input" field and type the desired message for that line. Use the space bar to center the text.

Line 1:
Line 2: **Welcome to the**
Line 3:
Line 4: **American Heritage**
Line 5:
Line 6: **Villa Apartments**
Line 7:

8. Click on the **Done** button. The "Edit/View Banner Message1 with small font" window will appear.
9. Edit the same lines as in the large font. The finished window should appear similar to Figure 10-11.

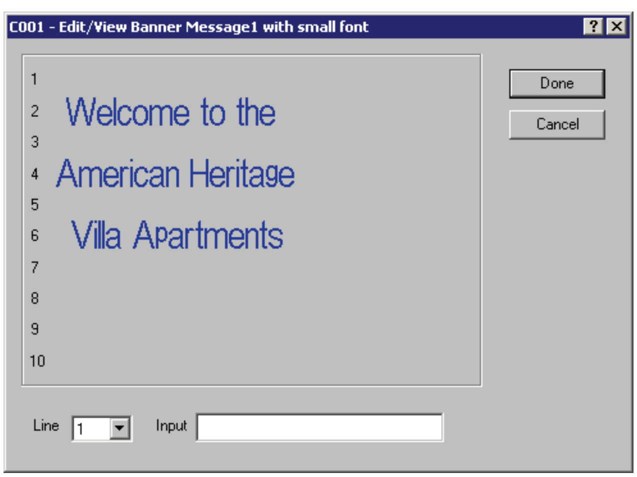


Figure 10-11: Edit/View Platinum Banner Message1 Window - Small Font

10. Click on the 

button.
11. Repeat steps 3-10 for messages 2 and 3.

EntraGuard Platinum Banner Message2 Default

Line 1: **Press the ARROW**
Line 2: **keys to find a name**
Line 3:
Line 4: **Hold the key down**
Line 5: **to scroll faster to**
Line 6: **find a tenant's name**
Line 7:

EntraGuard Platinum Banner Message3 Default

Line 1:
Line 2: **Press the CALL**
Line 3: **button to dial the**
Line 4: **tenant or press CLR**
Line 5: **to start again**
Line 6:
Line 7:

12. Once all the banner messages have been entered, click on the 

button to save these changes. If the banner messages are not saved before clicking any other button or exiting the System Setup window, the data entered is lost and must be re-entered.

13. You must update the access control network with the new information. Click on the 

button on the tool bar (for details on the update process refer to "Update the Network" on page 35 in section 5).

4.0 Setup Access Groups

A new icon has been added to the Setup Access Window for the EntraGuard Telephone Entry Controller. If an EntraGuard controller has been detected during autoconfiguration, the icon will appear as . When a time zone is associated with this controller in an access group, the time zone will affect when users are allowed access through the EntraGuard controlled door. For setup instructions see "Setup Access Groups" on page 12 in section 10.

5.0 Setup Users

Each person to be granted access to secured areas using an EntraGuard controller will need a User ID assigned to them. If a mixed PXL/EntraGuard system is in use, each person may have assigned to them both a card and a User ID.

Through the Setup Users menu, an operator can enroll, void, and delete User IDs/cards/PINs; assign User IDs/cards/PINs to users; enter and edit user information, including personal data fields; and apply access groups to users. Once User IDs/cards/PINs are enrolled, operators may use either the dialog box method or spreadsheet method for entering user data. The dialog box method ("User Data – Dialog Box Method" on page 13 in section 4) allows an operator to enter all user data through a series of "fill-in-the-blank" type windows. The spreadsheet method (see "User Data – Spreadsheet Method" on page 22 in section 4) allows an operator to enter all user data into a spreadsheet.

5.1 User Enrollment

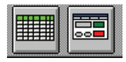
The following sections will direct you how to enroll users depending on the kind of system installed. Take a minute and determine what kind of access control system is in use.

- User ID only - when users need access to doors controlled by only EntraGuard controllers
- Card and User ID - when users need access to doors controlled by both an EntraGuard and PXL controller
- Card only (including Card+PIN) - when users need access to doors controlled by only PXL controllers (for enrolling card only or Card+PIN, see "Card Enrollment" on page 3 in section 4)

NOTE: Enrollment options selected previously will determine the options available to you as you begin enrollment. It is important that you verify those selections match the enrollment about to take place (see "Select Enrollment Options" on page 4 of this section).

5.1.1 Enroll User IDs Only

If the only controllers on your system are EntraGuard Telephone Entry controllers, each user will need to be assigned a User ID. The following instructions are based on the assumption that the “Only Use EntraGuard IDs” option was selected (see “Select Enrollment Options” on page 4 of this section).

1. To enroll User IDs, click on the Setup ⇒ Users pull-down menu or click on the  tool bar button. These two icons  are added to the tool bar and the Setup Users spreadsheet window appears (see Figure 10-12 on page 13 of this section). If the setup users spreadsheet window is not visible, click on the  tool bar button.

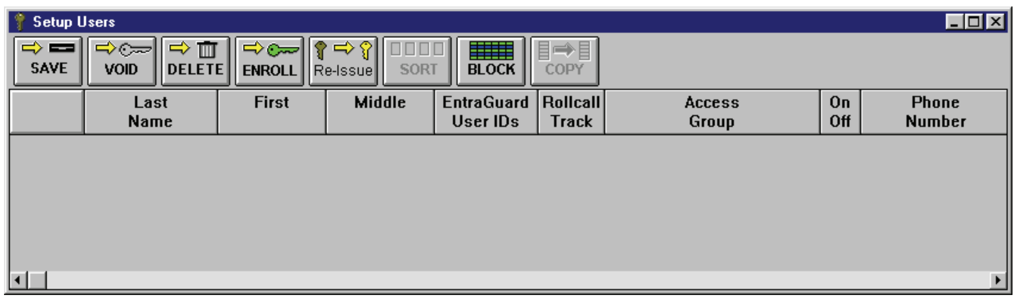
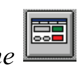


Figure 10-12: Setup Users Spreadsheet Window - EntraGuard User IDs Only

NOTE: If the Setup Users window does not display the EntraGuard User IDs column, click on the  *button, select the Preferences tab, and verify the Show EntraGuard IDs check box has a check in it. If there is no check, click on the check box and a check will appear allowing the column to be displayed. Make sure all the other check boxes are empty as none of them apply to EntraGuard only systems.*

2. Click on the  button. If the *Doors* program is not connected to the access control network, the program will automatically connect. The Enroll EntraGuard User IDs window appears (see Figure 10-13).

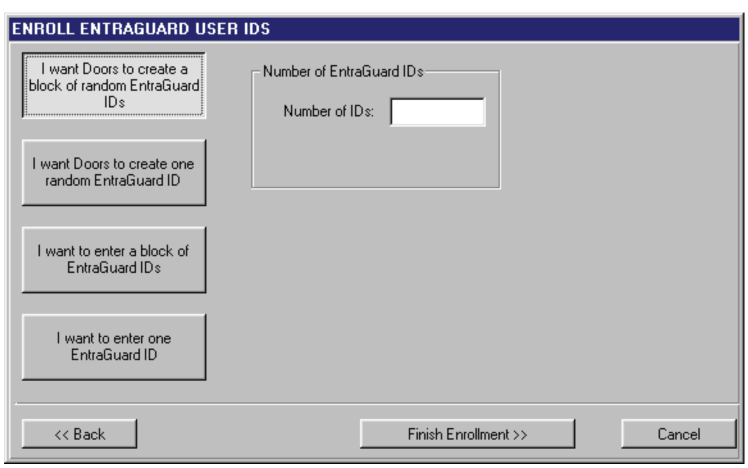


Figure 10-13: Enroll EntraGuard User IDs

3. Make a selection from the four buttons on the left according to your enrollment needs and the information given below.

Enroll a Block of Random User IDs

1. To enroll a block of randomly generated User IDs, click on the  button. The Enroll EntraGuard User IDs window will reveal the following field (see Figure 10-14).

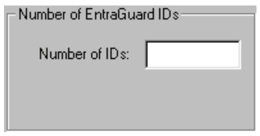
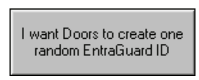


Figure 10-14: Enroll a Block of Random User IDs Field

2. In the "Number of IDs" cell, enter the number of users needing a randomly generated User ID. If new User IDs need to be enrolled for 5 users, the number 5 should be typed in the field.
3. Click on the  button. Skip to "Verify Enrollment of User IDs" on page 16 of this section.

Enroll One Random User ID

1. To enroll one randomly generated User ID, click on the  button. The Enroll EntraGuard User IDs window will reveal the following field (see Figure 10-15).

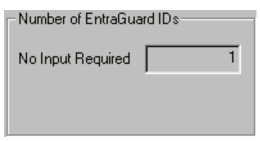


Figure 10-15: Enroll One Random User ID Field

2. This option will automatically enroll one randomly generated User ID.
3. Click on the  button. Skip to "Verify Enrollment of User IDs" on page 16 of this section.

Enroll a Block of User IDs

1. To enroll a block of operator assigned User IDs, click on the 

button. The Enroll EntraGuard User IDs window will reveal the following field (see Figure 10-16).

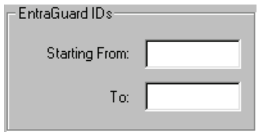


Figure 10-16: Enroll a Block of User IDs Field

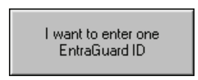
2. Click in the "Starting From" field, and enter the first User ID to be enrolled (the lowest number).
3. Click in the "To" field, and enter the last user ID to be enrolled (the highest number).

NOTE: The number of digits will be limited to the number selected when enabling the EntraGuard feature (see "Select Directory Code and User ID Digits" on page 4 of this section).

4. Click on the 

button. Skip to "Verify Enrollment of User IDs" on page 16 of this section.

Enroll One User ID

1. To enroll one operator assigned User ID, click on the 

button. The Enroll EntraGuard User IDs window will reveal the following field (see Figure 10-17.

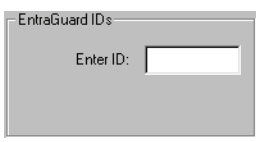


Figure 10-17: Enroll One User ID Field

2. Click in the "Enter ID" field and enter in the User ID to be enrolled for one user.

NOTE: The number of digits will be limited to the number selected when enabling the EntraGuard feature (see "Select Directory Code and User ID Digits" on page 4 of this section.

3. Click on the 

button. Skip to "Verify Enrollment of User IDs" on page 16 of this section.

5.1.1.1 Verify Enrollment of User IDs

1. Once you have made your enrollment selections and clicked on the 

button, the Enroll New Users confirmation window will appear (see Figure 10-18).

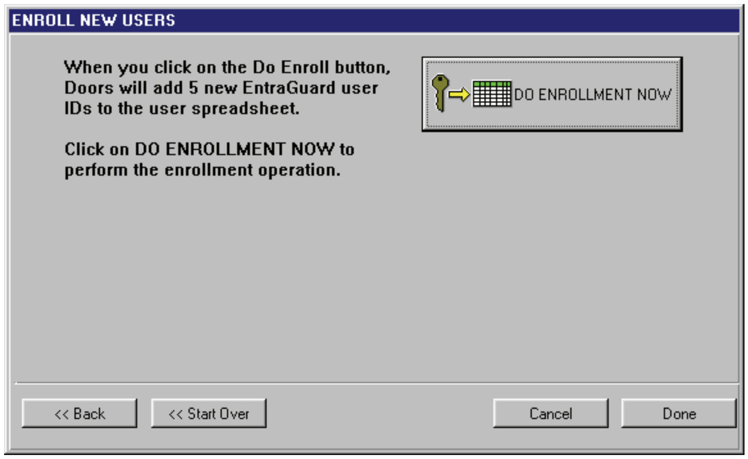


Figure 10-18: Enroll New Users Confirmation Window

2. The confirmation display shows the number of User IDs you are about to enroll. Take a moment to verify this number is correct. If this number is incorrect, click on the 

button or the 

button to return to the Enroll EntraGuard User IDs window to make changes.
3. Once you have verified all the information is correct on the confirmation display, click on the 

button. The User IDs are enrolled and the enrollment results are displayed (see Figure 10-19 on page 16 of this section).

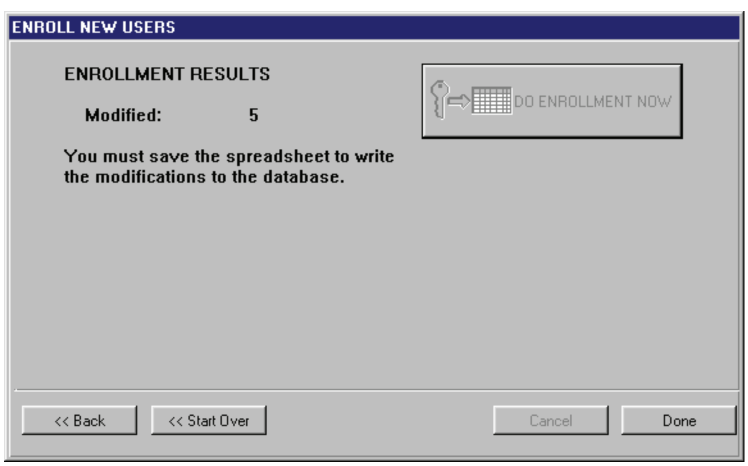
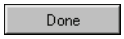


Figure 10-19: Enrollment Results Window

4. Carefully examine the information displayed under Enrollment Results. This field will alert you to the number of User IDs that were successfully enrolled and if there were any duplicate User IDs.

NOTE: If more than 100 User IDs are being enrolled at one time, the enrollment results display will show the enrollment of User IDs increase in increments of 100 until the database slots for all User IDs being enrolled have been created.

5. Click on the 

button to close the Enroll New Users window. The setup users spreadsheet window now contains the newly enrolled User IDs (see Figure 10-20).

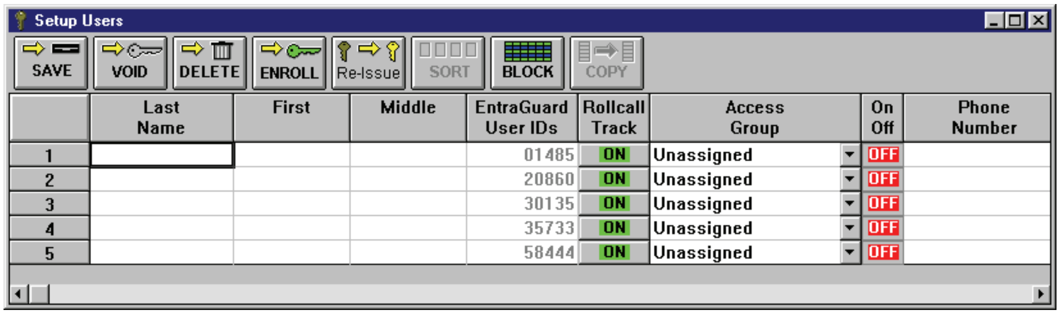


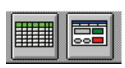
Figure 10-20: Setup Users Spreadsheet Window With Block Random Enrolled User IDs

6. Click on the 

button to save the enrollment. If the User ID enrollment information is not saved before clicking any other button or exiting the Setup Users window, the data entered is lost and must be re-entered.

5.1.2 Enroll Cards and User IDs

For mixed PXL/EntraGuard access control systems, each user may need to be assigned both a card and a User ID in order to gain access to all areas of the network. The following instructions are based on the assumption that the "Use Both Cards and EntraGuard IDs" option was selected previously (see "Select Enrollment Options" on page 4 of this section).

1. To enroll cards and User IDs, click on the Setup ⇒ Users pull-down menu or click on the  tool bar button. These two icons  are added to the tool bar and the Setup Users spreadsheet window appears (see Figure 10-21). If the setup users spreadsheet window is not visible, click on the  tool bar button.

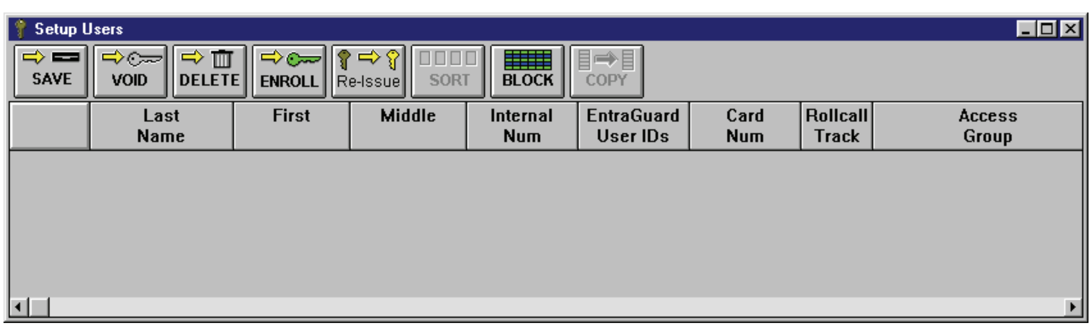


Figure 10-21: Setup Users Spreadsheet Window - Cards and EntraGuard User IDs

NOTE: If the Setup Users window does not display the Internal Num, EntraGuard User IDs, and Card Num columns, click on the  *button, select the Preferences tab, and verify the Show Card Numbers, Show Internal Card Numbers, and Show EntraGuard IDs check boxes have checks in them. If any of the boxes do not have a check in them, click on the check box and a check will appear allowing the column to be displayed.*

2. Click on the  button. If the *Doors* program is not connected to the access control network, the program will automatically connect. The Select Enrollment Method window appears (see Figure 10-22).

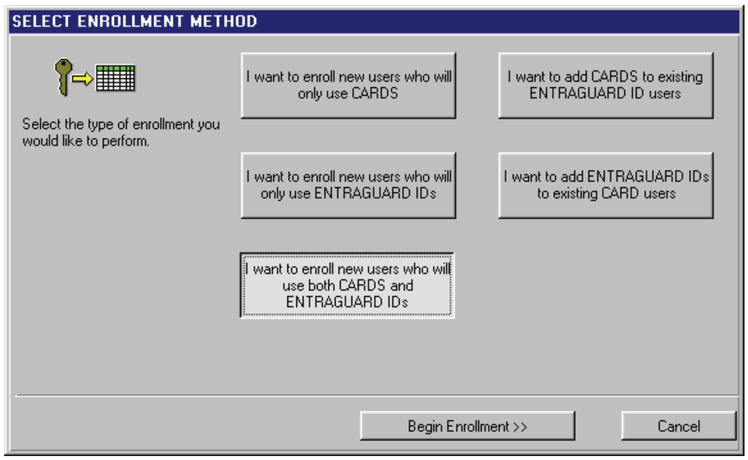


Figure 10-22: Select Enrollment Method Window - Cards and User IDs Selected

3. Click on the  button for enrollment of cards and EntraGuard User IDs. Then click on the  button. The Enroll Cards window appears (see Figure 10-23).

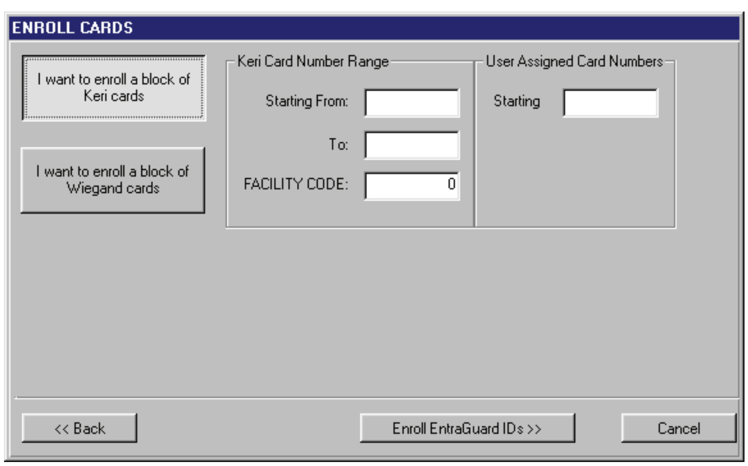
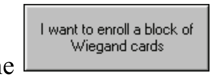


Figure 10-23: Enroll Cards Window

4. If the cards to be enrolled are Keri Proximity cards, click on the 

button.
5. If the cards to be enrolled are 26-bit Wiegand cards, click on the 

button.

NOTE: Once the EntraGuard feature is enabled, enrollment of cards by presentation to a reader is no longer available.

6. Locate the Keri/Wiegand Card Number Range field. Click in the **Starting From** field. Enter the card number for the first card in the range of cards to be enrolled (the lowest number). The card number is the second set of digits printed on the body of the card (in Figure 10-24, it is the digits corresponding to 187491). The card number will be more than 4 digits long. For example, the entire number of the first card is K1757 187491; the card number is **187491**, 6 digits long.

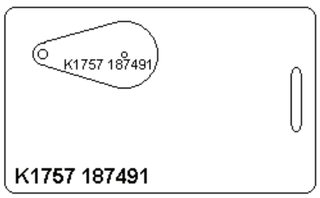


Figure 10-24: Proximity Card/Key Tag Number

7. Locate the Keri/Wiegand Card Number Range field. Click in the **To** field. Enter the card number for the last card in the range of cards to be enrolled (the highest number).
8. Locate the Facility Code field. Click in the **FACILITY CODE** field and enter the facility code for the cards. The default facility code value is 0 (zero).

*NOTE: For Keri Proximity cards, facility codes may range from 0 to 31. For 26-bit Wiegand cards, facility codes may range from 0 to 255. The facility code is programmed into each card. To enroll cards, you **must** know the facility code programmed into the card. If you do not know the facility code for the cards you are enrolling, please contact your card supplier for the facility code number **before** continuing the card enrollment process.*

NOTE: If you are block enrolling non-Keri Wiegand cards, be sure you know the actual internal card numbers programmed into the cards and verify the internal numbers are in consecutive order. Using incorrect numbers and non-consecutive cards invalidate the block enrollment process.

9. The default for User Assigned Card Numbers is to copy the card number from the Keri/Wiegand Card Number Range field. If there is a need for user assigned card numbers that are different from the card number printed on the body of the card, locate the User Assigned Card Numbers field. Click in the **Starting** field. Enter the user assigned number for the first card in the set. Numbers for the remaining cards will be assigned in ascending, sequential order from the first number.

10. The resulting window should look similar to Figure 10-25.

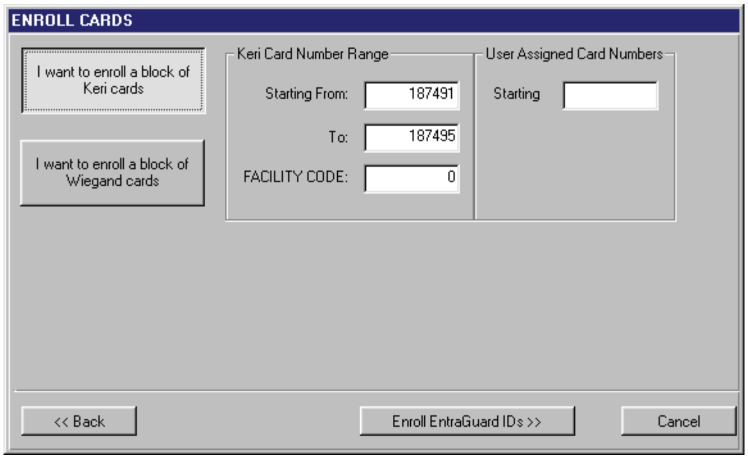
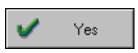
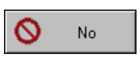


Figure 10-25: Enroll Cards Window - Block Enrollment

11. Click on the 

button.

NOTE: If a large number of cards are being enrolled (greater than 5,000 cards at one time), it can take some time for the enrollment process to complete. A card quantity verification window appears (see Figure 10-26) to warn the operator of the time involved in enrolling a large number of cards at one time. Click on the 

button to continue with the enrollment. If the number of cards being enrolled is incorrect, or if you do not want to enroll such a large number of cards at one time, click on the 

button.

NOTE: Entering a large amount of cards by mistake (i.e 30,000) may be more than the host computer is able to handle.

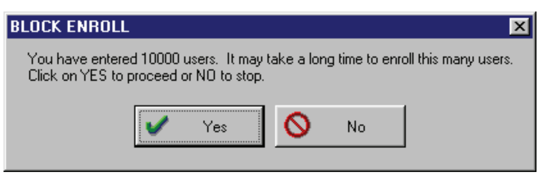


Figure 10-26: Block Enrollment Card Quantity Verification Window

12. The Enroll EntraGuard User IDs window appears (see Figure 10-27 on page 21 of this section).

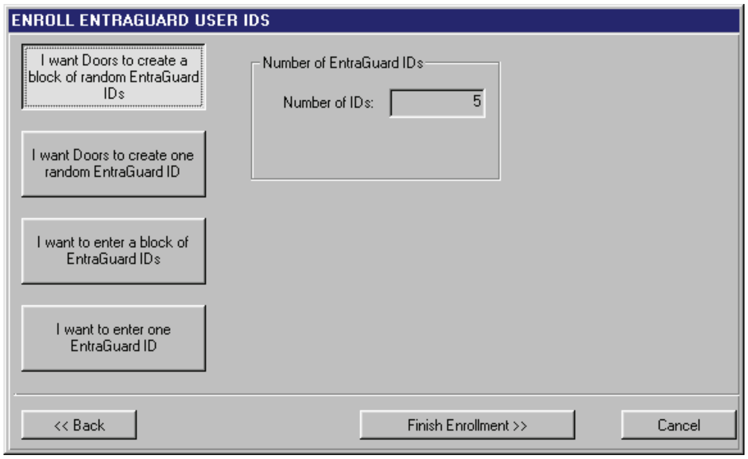
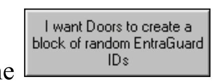


Figure 10-27: Enroll EntraGuard User IDs with Cards

13. Make a selection from the four buttons on the left according to your enrollment needs and the information given below.

Enroll a Block of Random User IDs

1. To enroll a block of randomly generated User IDs, click on the 

button. Since these EntraGuard User IDs are being enrolled in connection with access cards, the number of randomly generated User IDs is pre-selected based on the number of cards enrolled in the previous window.
2. Click on the 

button. Skip to “Verify Enrollment of Cards and User IDs” on page 22 of this section.

Enroll One Random User ID

NOTE: This button should not be used unless only one card has been enrolled. Selecting this button will cause only one user to be enrolled regardless of the information entered in the Enroll Cards window.

Enroll a Block of User IDs

1. To enroll a block of operator assigned User IDs, click on the 

button. The Enroll EntraGuard User IDs window will reveal the following field (see Figure 10-28).

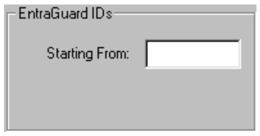


Figure 10-28: Enroll a Block of User IDs with Cards Field

2. Click in the “Starting From” field and enter the first User ID to be enrolled (the lowest number). The *Doors* program will automatically fill in the User IDs for the remainder of the enrolled cards in increments of one.

NOTE: The number of digits will be limited to the number selected when enabling the EntraGuard feature (see “Select Directory Code and User ID Digits” on page 4 of this section).

3. Click on the 

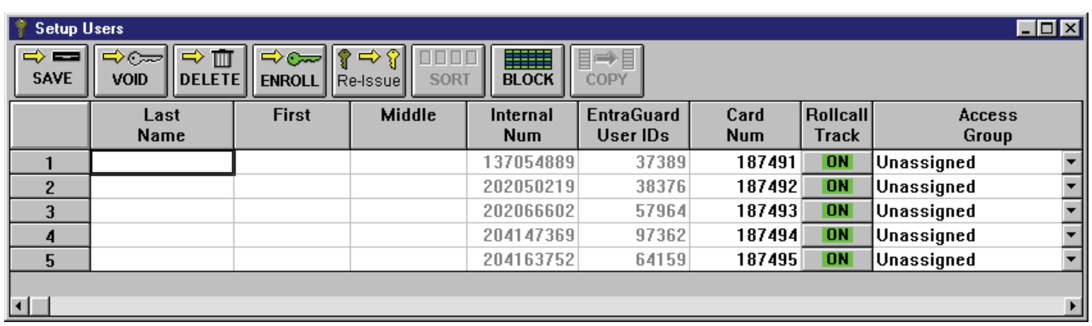
button. Skip to “Verify Enrollment of Cards and User IDs” on page 22 of this section.

Enroll One User ID

NOTE: This button should not be used unless only one card has been enrolled. Selecting this button will cause only one user to be enrolled regardless of the information entered in the Enroll Cards window.

5.1.2.1 Verify Enrollment of Cards and User IDs

1. Once you have made your enrollment selections, follow the instructions given in “Verify Enrollment of User IDs” on page 16 of this section. After completing the verification and enrollment process, the Setup Users spreadsheet window will contain the newly enrolled cards and User IDs (see Figure 10-29).



	Last Name	First	Middle	Internal Num	EntraGuard User IDs	Card Num	Rollcall Track	Access Group
1				137054889	37389	187491	ON	Unassigned
2				202050219	38376	187492	ON	Unassigned
3				202066602	57964	187493	ON	Unassigned
4				204147369	97362	187494	ON	Unassigned
5				204163752	64159	187495	ON	Unassigned

Figure 10-29: Setup Users Spreadsheet Window With Cards and User IDs Enrolled

2. Click on the 

button to save the enrollment. If the card and User ID enrollment information is not saved before clicking any other button or exiting the Setup Users window, the data entered is lost and must be re-entered.

5.1.3 Add User IDs to Previously Enrolled Cards

In some cases User IDs may need to be enrolled for users who already have cards assigned to them (for instance when an already existing system adds an EntraGuard controller).

NOTE: Make sure either the "Use Both Cards and EntraGuard IDs" option or the "Only Use EntraGuard IDs" option is selected (see "Select Enrollment Options" on page 4 of this section). If the "Only Use Cards" option is selected, enrollment of EntraGuard IDs will not be possible.

1. To add User IDs to users with previously enrolled cards, click on the Setup ⇒ Users pull-down menu or click on the  tool bar button. These two icons  are added to the tool bar and the Setup Users spreadsheet window appears (see Figure 10-30). If the setup users spreadsheet window is not visible, click on the  tool bar button.
2. The existing database should be visible with all previously enrolled users and their card information (see Figure 10-30).

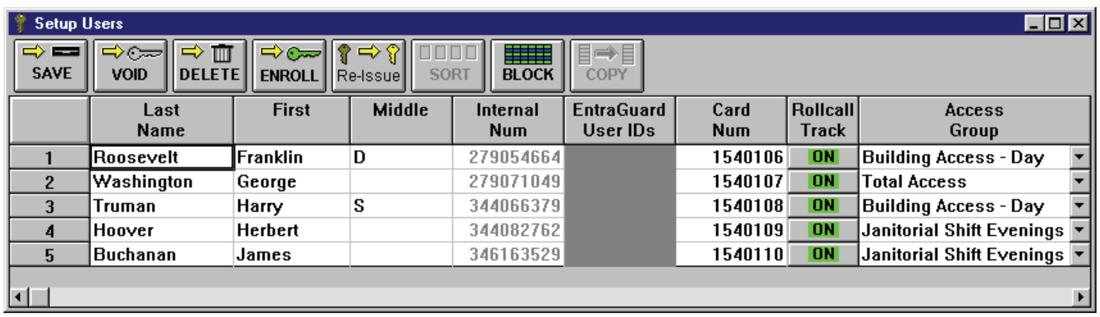


Figure 10-30: Setup Users Spreadsheet Window with Existing Card Users

NOTE: If the Setup Users window does not display the EntraGuard User IDs column, click on the  *button, select the Preferences tab, and verify the Show EntraGuard IDs check box has a check in it. If there is no check, click on the check box and a check will appear allowing the column to be displayed.*

3. Click on the  button. If the *Doors* program is not connected to the access control network, the program will automatically connect. The Select Enrollment Method window appears (see Figure 10-31 on page 24 of this section).

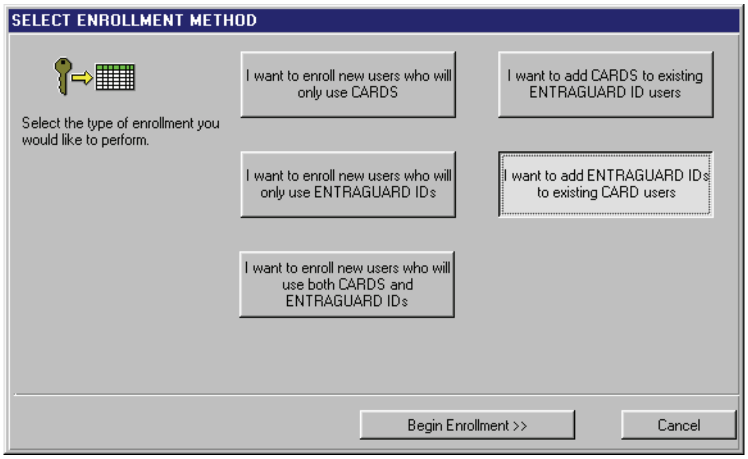


Figure 10-31: Select Enrollment Method Window - Add EntraGuard User IDs

4. Click on the 

button to add EntraGuard User IDs to existing card users. Then click on the 

button. The Enroll EntraGuard User IDs window appears (see Figure 10-13).

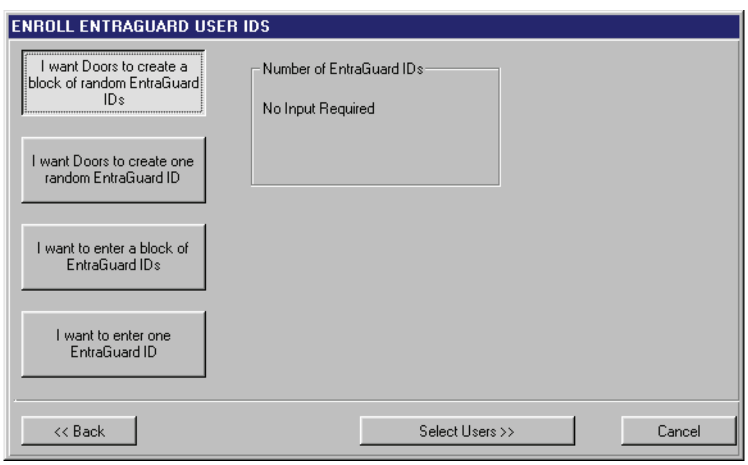
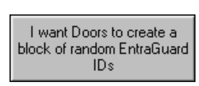
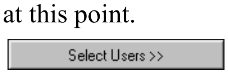


Figure 10-32: Add EntraGuard User IDs to Existing Card Users

5. Make a selection from the four buttons on the left according to your enrollment needs and the information given below.

Enroll a Block of Random User IDs

1. To enroll a block of randomly generated User IDs, click on the 

button. No input is necessary at this point.
2. Click on the 

button. Skip to "Select Users To Add EntraGuard IDs" on page 26 of this section.

Enroll One Random User ID

1. To enroll one randomly generated User ID, click on the  button. No input is necessary at this point.
2. Click on the  button. Skip to “Select Users To Add EntraGuard IDs” on page 26 of this section.

Enroll a Block of User IDs

1. To enroll a block of operator assigned User IDs, click on the  button. The Enroll EntraGuard User IDs window will reveal the following field (see Figure 10-33).

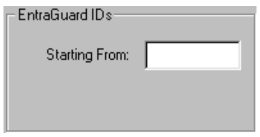


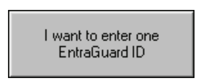
Figure 10-33: Enroll a Block of User IDs To Existing Card Users Field

1. Click in the “Starting From” field, and enter the first user ID to be enrolled (the lowest number). In the next step selection of the users to be assigned a User ID will take place. The *Doors* program will automatically fill the User IDs for the remainder of the enrolled users in increments of one.

NOTE: The number of digits will be limited to the number selected when enabling the EntraGuard feature (see “Select Directory Code and User ID Digits” on page 4 of this section).

2. Click on the  button. Skip to “Select Users To Add EntraGuard IDs” on page 26 of this section.

Enroll One User ID

1. To enroll one operator assigned User ID, click on the  button. The Enroll EntraGuard User IDs window will reveal the following field (see Figure 10-34).

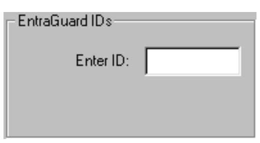


Figure 10-34: Enroll One User ID Field

2. Click in the “Enter ID” field and enter in the User ID to be enrolled for one user.

NOTE: The number of digits will be limited to the number selected when enabling the EntraGuard feature (see “Select Directory Code and User ID Digits” on page 4 of this section).

3. Click on the  button. Skip to “Select Users To Add EntraGuard IDs” on page 26 of this section.

5.1.3.1 Select Users To Add EntraGuard IDs

1. Once you have made your enrollment selections and clicked on the 

button, the Add EntraGuard IDs To Card Users window will appear (see Figure 10-35).

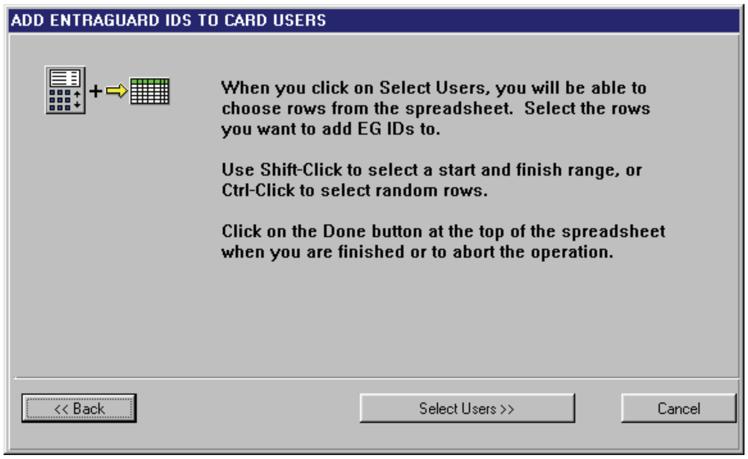


Figure 10-35: Add EntraGuard IDs To Card Users Window

2. Click on the 

button. The Setup Users spreadsheet window will appear (see Figure 10-36). Any users already assigned a User ID will not be visible.

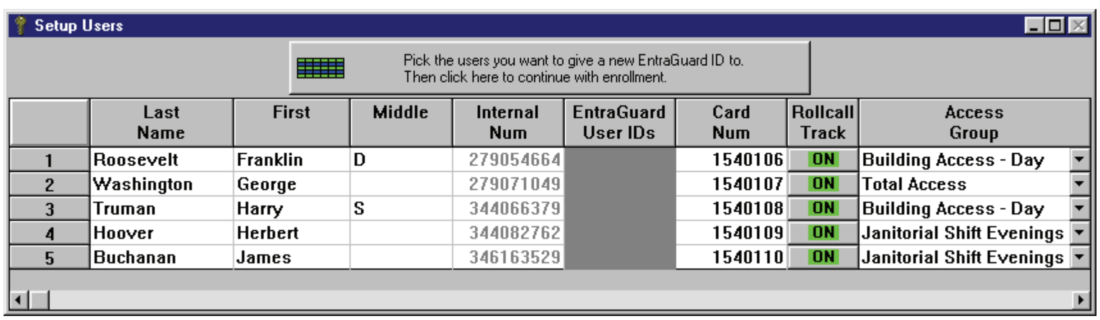


Figure 10-36: Setup Users - Select Users For User ID Addition

3. Click on the users to be assigned a User ID. There are three ways to select the users to which a User ID should be assigned. Use the method you find easiest (see Figure 10-37 on page 27 of this section).

   - Click and hold on the row of the first user to be assigned a User ID and drag the mouse down to the row of the last user.
   - Click on the row of the first user to be assigned a User ID, hold the Shift key down, and click on the row of the last user.
   - Hold the Ctrl key down and one-at-a-time click on the rows of each user to be assigned a User ID. This method is best used when the users are not in sequential order.

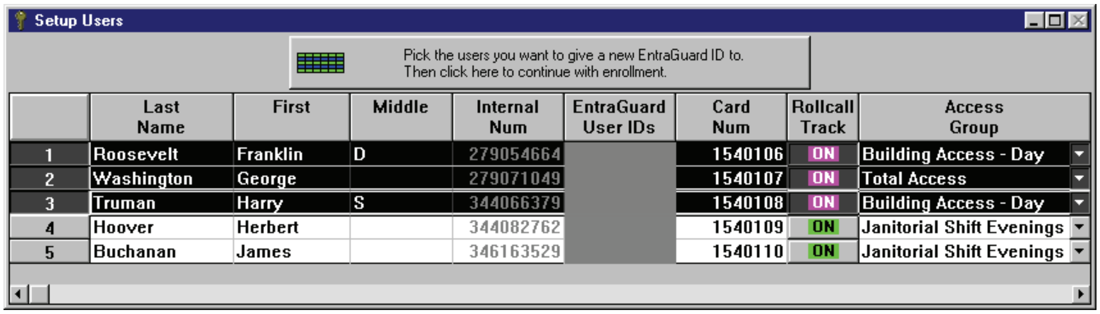
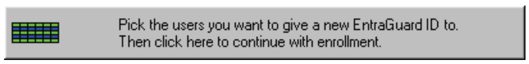


Figure 10-37: Setup Users - Selected Users for User ID Addition

4. Once all the users to be assigned a User ID have been selected, click on the 

button. The Enroll New Users window will appear (see Figure 10-38).

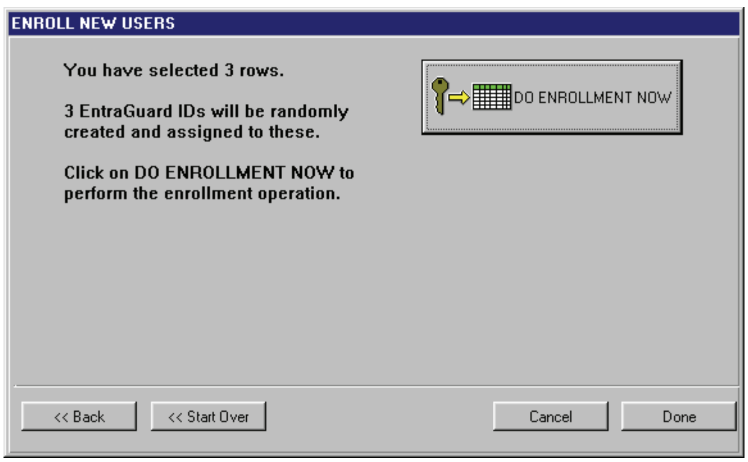
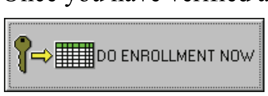


Figure 10-38: Enroll New Users Confirmation Window When Adding User IDs

5. The confirmation display shows the number of User IDs you are about to enroll. Take a moment to verify this number is correct. If this number is incorrect, click on the 

button to return to the Add EntraGuard IDs To Card Users window (see Figure 10-35 on page 26 of this section), or the 

button to return to the Select Enrollment Method window (see Figure 10-31 on page 24 of this section).
6. Once you have verified all the information is correct on the confirmation display, click on the 

button. The User IDs are assigned to the selected spreadsheet rows and the enrollment results are displayed (see Figure 10-39 on page 28 of this section).

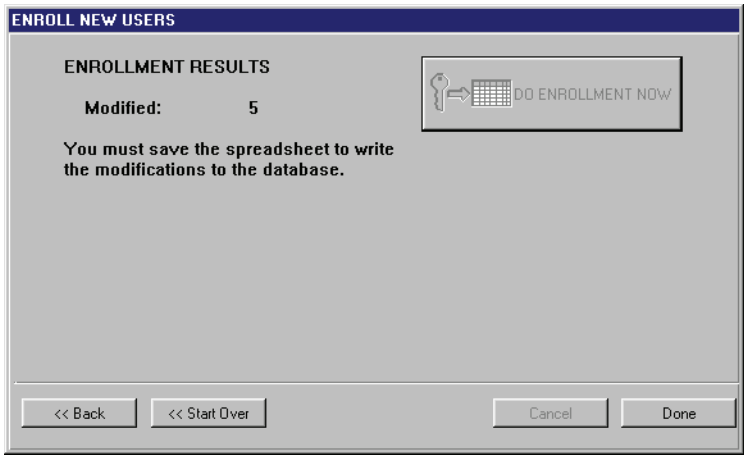


Figure 10-39: Enrollment Results Window

7. Carefully examine the information displayed under Enrollment Results.
8. Click on the  button to close the Enroll New Users window. The setup users spreadsheet window now contains the newly enrolled User IDs (see Figure 10-40).

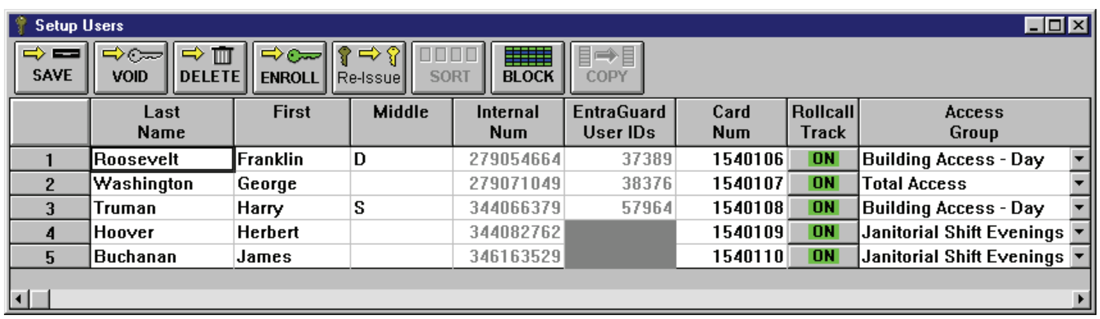


Figure 10-40: Setup Users Spreadsheet Window With User IDs Added To Card Users

9. Click on the  button to save the enrollment. If the enrollment information is not saved before clicking any other button or exiting the Setup Users window, the data entered is lost and must be re-entered.

5.1.4 Add Cards to Previously Enrolled User IDs

In some cases cards may need to be enrolled for users who already have User IDs assigned to them (for instance when an already existing EntraGuard system adds a PXL controller).

NOTE: Make sure wither the "Use Both Cards and EntraGuard IDs" option or the "Only Use Cards" option is selected (see "Select Enrollment Options" on page 4 of this section). If the "Only Use EntraGuard IDs" option is selected, enrollment of cards will not be possible.

1. To add cards to users with previously enrolled User IDs, click on the Setup ⇒ Users pull-down menu or click on the  tool bar button. These two icons  are added to the tool bar and the Setup Users spreadsheet window appears (see Figure 10-41). If the setup users spreadsheet window is not visible, click on the  tool bar button.
2. The existing database should be visible with all previously enrolled users and their User ID information (see Figure 10-41).

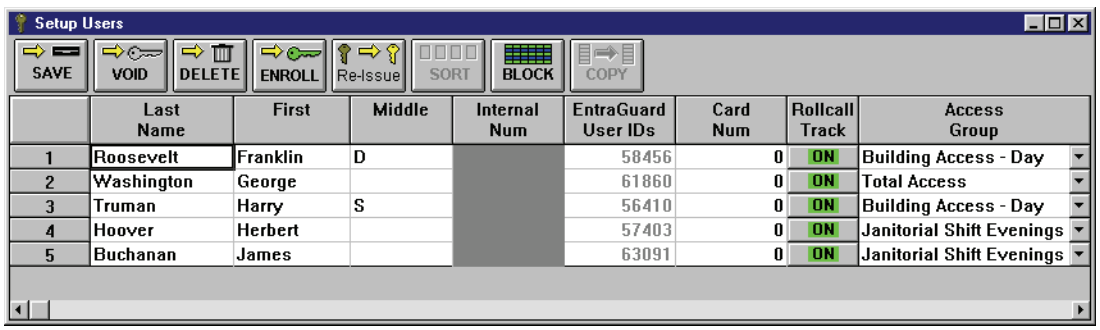


Figure 10-41: Setup Users Spreadsheet Window with Existing User IDs

NOTE: If the Setup Users window does not display the Internal Num and Card Num columns, click on the  button, select the Preferences tab, and verify the Show Internal Card Numbers and Show Card Numbers check boxes have checks in them. If there is no check, click on each check box and a check will appear allowing the columns to be displayed.

3. Click on the  button. If the *Doors* program is not connected to the access control network, the program will automatically connect. The Select Enrollment Method window appears (see Figure 10-42 on page 30 of this section).

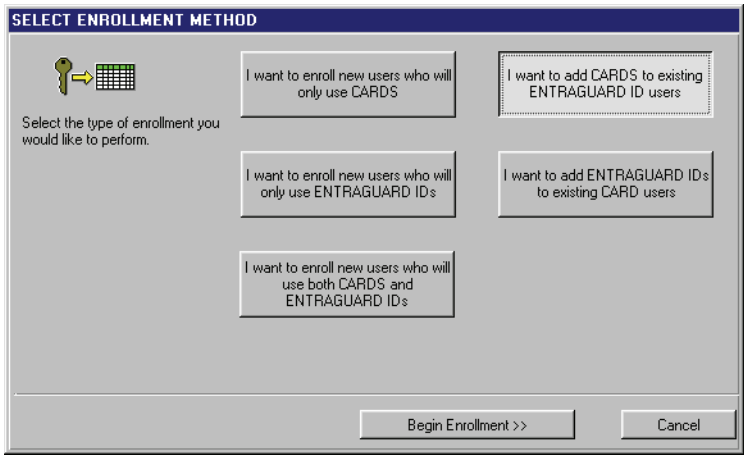


Figure 10-42: Select Enrollment Method Window - Add Cards

4. Click on the 

button. Then click on the 

button. The Enroll Cards window appears (see Figure 10-43).

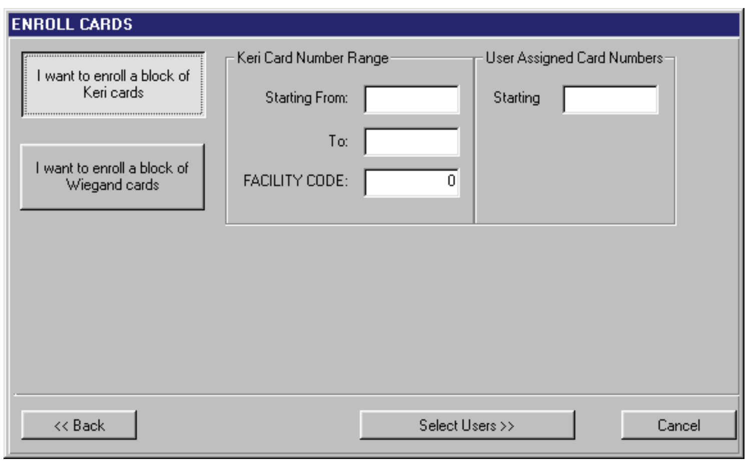
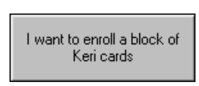
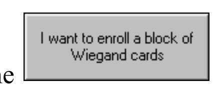


Figure 10-43: Add Cards to Existing EntraGuard IDs

5. If the cards to be enrolled are Keri Proximity cards, click on the 

button.

6. If the cards to be enrolled are 26-bit Wiegand cards, click on the 

button.

NOTE: Once the EntraGuard feature is enabled, enrollment of cards by presentation to a reader is no longer available.

7. Locate the Keri/Wiegand Card Number Range field. Click in the **Starting From** field. Enter the card number for the first card in the range of cards to be enrolled (the lowest number). The card number is the second set of digits printed on the body of the card (in Figure 10-44 on page 31 of this section, it is the digits corresponding to 187491). The card number will be more than 4 digits long. For example, the entire number of the first card is K1757 187491; the card number is **187491**, 6 digits long.

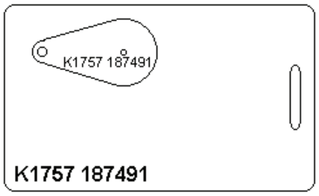


Figure 10-44: Proximity Card/Key Tag Number

8. Locate the Keri/Wiegand Card Number Range field. Click in the **To** field. Enter the card number for the last card in the range of cards to be enrolled (the highest number).
9. Locate the Facility Code field. Click in the **FACILITY CODE** field and enter the facility code for the cards. The default facility code value is 0 (zero).

*NOTE: For Keri Proximity cards, facility codes may range from 0 to 31. For 26-bit Wiegand cards, facility codes may range from 0 to 255. The facility code is programmed into each card. To enroll cards, you **must** know the facility code programmed into the card. If you do not know the facility code for the cards you are enrolling, please contact your card supplier for the facility code number **before** continuing the card enrollment process.*

NOTE: If you are block enrolling non-Keri Wiegand cards, be sure you know the actual internal card numbers programmed into the cards and verify the internal numbers are in consecutive order. Using incorrect numbers and non-consecutive cards invalidate the block enrollment process.

10. The default for User Assigned Card Numbers is to copy the card number from the Keri/Wiegand Card Number Range field. If there is a need for user assigned card numbers that are different from the card number printed on the body of the card, locate the User Assigned Card Numbers field. Click in the **Starting** field. Enter the user assigned number for the first card in the set. Numbers for the remaining cards will be assigned in ascending, sequential order from the first number.
11. The resulting window should look similar to Figure 10-45.

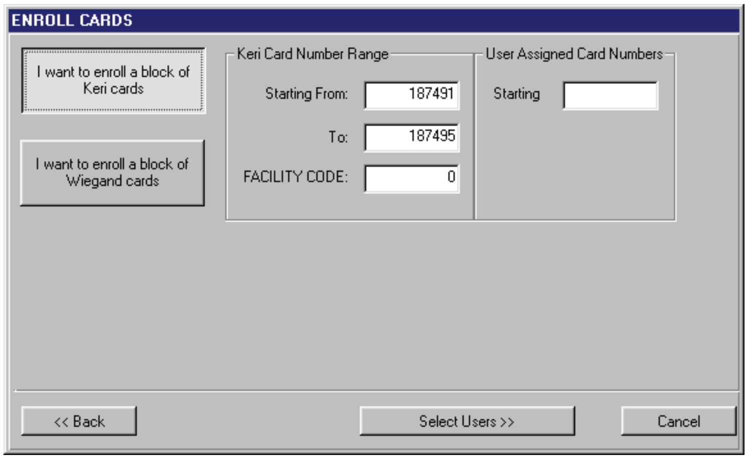
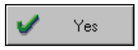


Figure 10-45: Enroll Cards Window - Add Cards To Existing EntraGuard IDs

12. Click on the  button.

NOTE: If a large number of cards are being enrolled (greater than 5,000 cards at one time), it can take some time for the enrollment process to complete. A card quantity verification window appears (see Figure 10-46) to warn the operator of the time involved in enrolling a large number of cards at one time. Click on the 

button to continue with the enrollment. If the number of cards being enrolled is incorrect, or if you do not want to enroll such a large number of cards at one time, click on the 

button.

NOTE: Entering a large amount of cards by mistake (i.e 30,000) may be more than the host computer is able to handle.

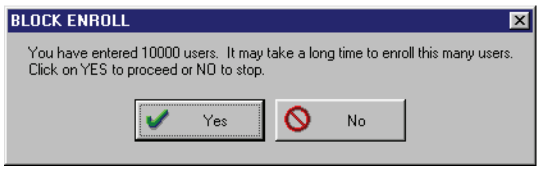


Figure 10-46: Block Enrollment Card Quantity Verification Window

5.1.4.1 Select Users To Add Cards

1. Once you have made your enrollment selections and clicked on the 

button, the Add Cards To EntraGuard Users window will appear (see Figure 10-47).

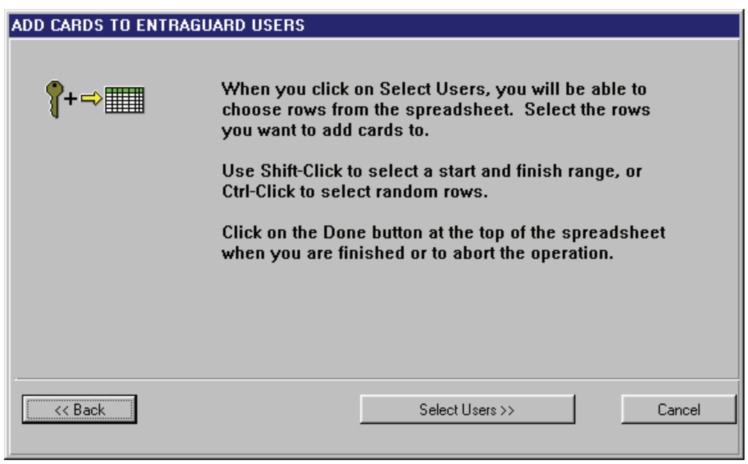
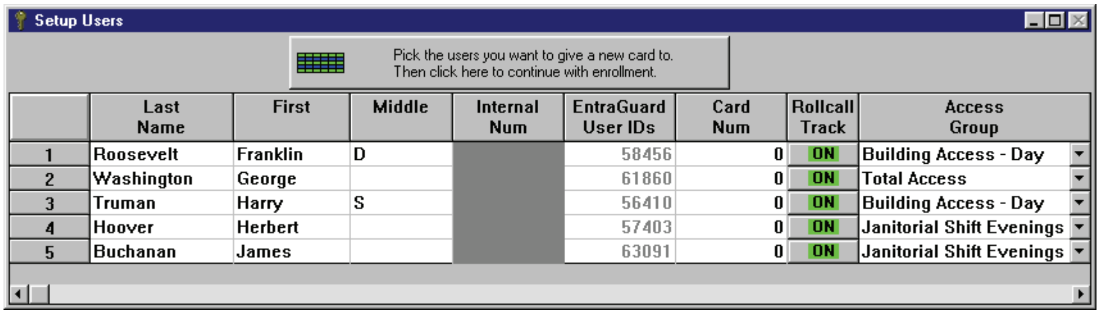


Figure 10-47: Add Cards To EntraGuard Users Window

2. Click on the 

button. The Setup Users spreadsheet window will appear (see Figure 10-48 on page 33 of this section). Any users already assigned a card will not be visible.

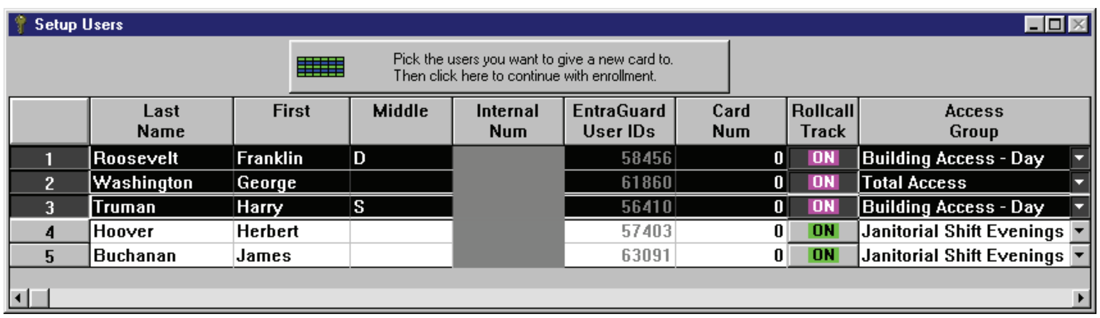


	Last Name	First	Middle	Internal Num	EntraGuard User IDs	Card Num	Rollcall Track	Access Group
1	Roosevelt	Franklin	D		58456	0	ON	Building Access - Day
2	Washington	George			61860	0	ON	Total Access
3	Truman	Harry	S		56410	0	ON	Building Access - Day
4	Hoover	Herbert			57403	0	ON	Janitorial Shift Evenings
5	Buchanan	James			63091	0	ON	Janitorial Shift Evenings

Figure 10-48: Setup Users Spreadsheet Window - Select Rows To Add Cards

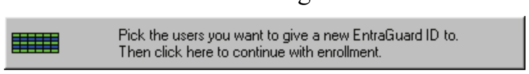
3. Click on the users to be assigned a card. There are three ways to select the users to which a card should be assigned. Use the method you find easiest (see Figure 10-49).

   - Click and hold on the row of the first user to be assigned a card and drag the mouse down to the row of the last user.
   - Click on the row of the first user to be assigned a card, hold the Shift key down, and click on the row of the last user.
   - Hold the Ctrl key down and one-at-a-time click on the rows of each user to be assigned a card. This method is best used when the users are not in sequential order.



	Last Name	First	Middle	Internal Num	EntraGuard User IDs	Card Num	Rollcall Track	Access Group
1	Roosevelt	Franklin	D		58456	0	ON	Building Access - Day
2	Washington	George			61860	0	ON	Total Access
3	Truman	Harry	S		56410	0	ON	Building Access - Day
4	Hoover	Herbert			57403	0	ON	Janitorial Shift Evenings
5	Buchanan	James			63091	0	ON	Janitorial Shift Evenings

Figure 10-49: Setup Users Spreadsheet Window - Selected Users for Card Addition

4. Once all the users to be assigned a card have been selected, click on the 

button. The Enroll New Users window will appear (see Figure 10-50 on page 34 of this section).

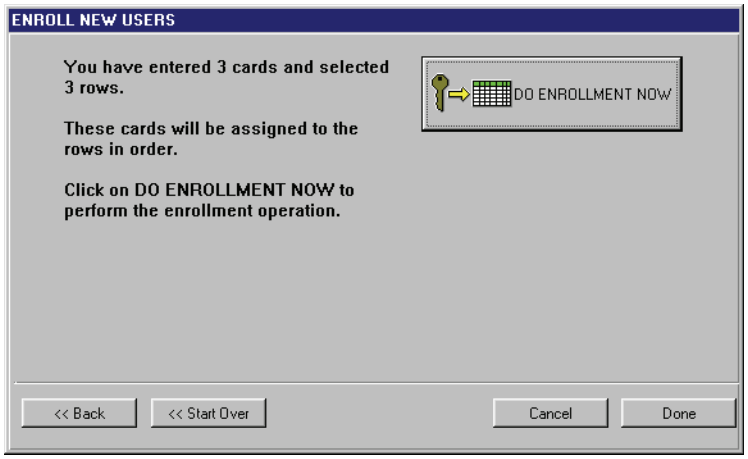


Figure 10-50: Enroll New Users Confirmation Window When Adding User IDs

5. The confirmation display shows the number of cards you are about to enroll. Take a moment to verify this number is correct. If this number is incorrect, click on the << Back button to return to the Add Cards To EntraGuard Users window (see Figure 10-35 on page 26 of this section), or the << Start Over button to return to the Select Enrollment Method window (see Figure 10-31 on page 24 of this section).
6. Once you have verified all the information is correct on the confirmation display, click on the DO ENROLLMENT NOW button. The cards are assigned to the selected spreadsheet rows and the enrollment results are displayed (see Figure 10-51).

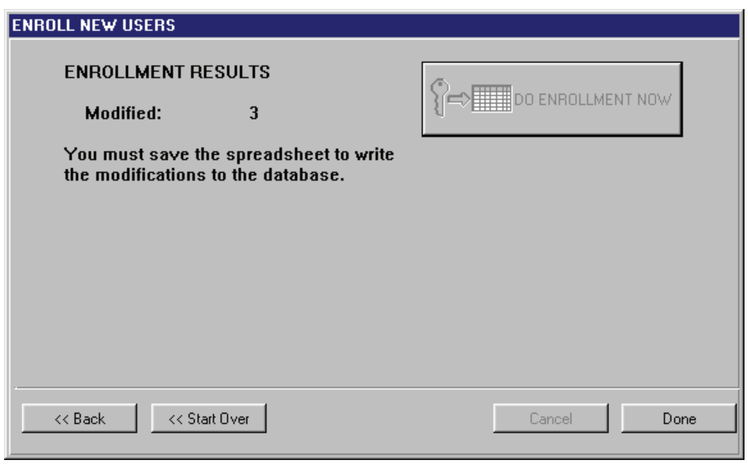
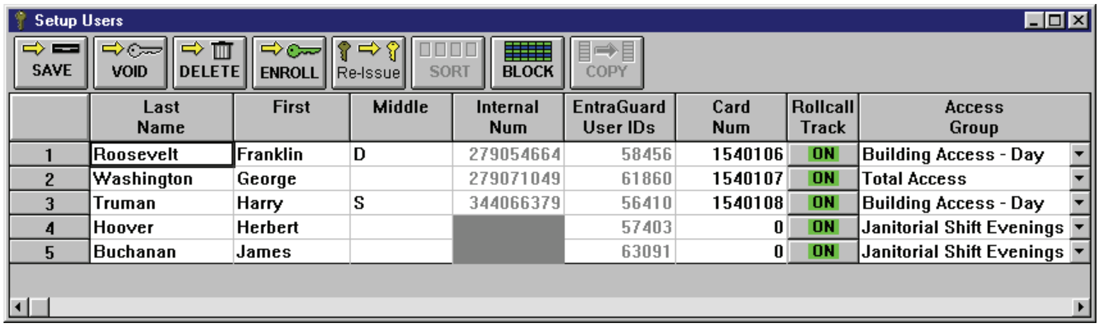


Figure 10-51: Enrollment Results Window - Cards Added

7. Carefully examine the information displayed under Enrollment Results.
8. Click on the Done button to close the Enroll New Users window. The Setup Users spreadsheet window now contains the newly enrolled cards (see Figure 10-52 on page 35 of this section).



	Last Name	First	Middle	Internal Num	EntraGuard User IDs	Card Num	Rollcall Track	Access Group
1	Roosevelt	Franklin	D	279054664	58456	1540106	ON	Building Access - Day
2	Washington	George		279071049	61860	1540107	ON	Total Access
3	Truman	Harry	S	344066379	56410	1540108	ON	Building Access - Day
4	Hoover	Herbert			57403	0	ON	Janitorial Shift Evenings
5	Buchanan	James			63091	0	ON	Janitorial Shift Evenings

Figure 10-52: Setup Users Spreadsheet Window With Cards Added to EntraGuard Users

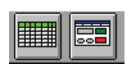
9. Click on the  button to save the enrollment. If the enrollment information is not saved before clicking any other button or exiting the Setup Users window, the data entered is lost and must be re-entered.

5.2 Entering EntraGuard User Data

Once the EntraGuard IDs have been enrolled, data may be entered or edited for all User IDs displayed in the spreadsheet.

5.2.1 User Data – Dialog Box Changes

When the EntraGuard feature is enabled in *Doors*, 5 new fields are added to the User Data tab to allow for data entry of necessary EntraGuard information. Leaving any of these fields blank may result in the EntraGuard unit not functioning properly. For more detail on the Dialog Box method of entering user data, see “User Data – Dialog Box Method” on page 13 in section 4.

1. To enter user data through the dialog box method, click on the Setup ⇒ Users pull-down menu or click on the  tool bar button. These two icons  are added to the tool bar and the Setup Users spreadsheet window appears.
2. Click on the  tool bar button to ensure the setup users dialog box window is active.
3. Click on the **User Data** tab. The User Data window appears (see Figure 10-53).

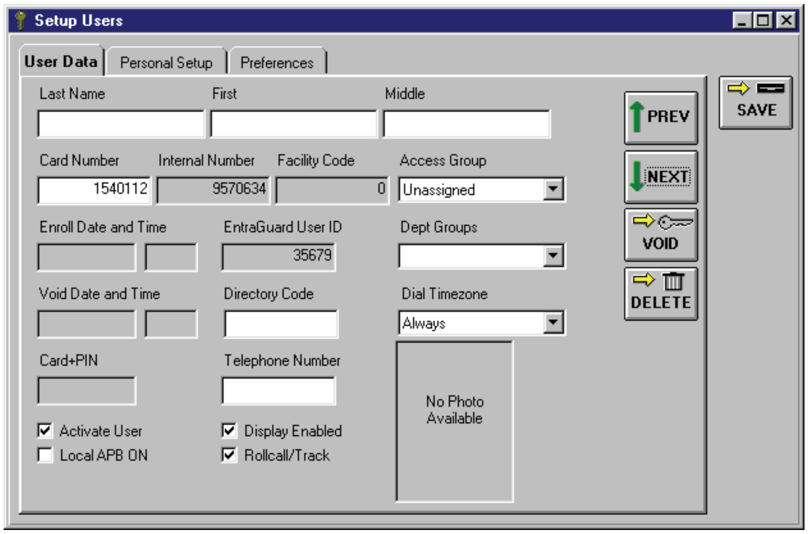


Figure 10-53: User Data Entry Window With New EntraGuard Fields

NOTE: The Card Number, Internal Number, Facility Code, Dept Groups, and EntraGuard User ID fields can be either visible or hidden depending on selections made on the Preferences tab. If one of these fields is not visible, click on the Preferences tab, and verify there is a check mark in the check box for the field you want displayed. If there is not check mark in the check box, this field will be hidden on the User Data tab.

4. The following 5 fields are added for use with an EntraGuard unit. The rest of the fields may be filled in according to the instructions given in "Entering User Data – Dialog Box Method" on page 13 in section 4.

   - EntraGuard User ID – This number is automatically entered during enrollment and is the code tenants must use to enter through an EntraGuard controlled door.
   - Directory Code – This number is assigned by the operator as the number visitors must dial from the EntraGuard unit to dial up a tenant to request entry. This number is limited to the number of digits assigned during "Select Directory Code and User ID Digits" on page 4 of this section.
   - Telephone Number – This is the tenant's telephone number. The phone number cell may hold up to 15 characters. If it is necessary to use an area code for the EntraGuard controller to dial up the tenant's phone, then that area code must be entered here (i.e. 1-800-555-3456).
   - Dial Timezone – This is the time zone assigned to the tenant determining when they will accept calls from visitors at the EntraGuard unit. To set up a time zone see "Setup Time Zones" on page 3 in section 3.
   - Display Enabled – A check in this check box allows a tenant's name to appear on the tenant listing on the EntraGuard LCD. If a tenant does not want their name to appear on the list, click on the check box and the check mark is removed. Removing the tenant's name from the listing does not disable the ability of visitors to dial the tenant.

5. Click on the 

button. If the user data is not saved before clicking any other button or exiting the User Data tab, the data entered is lost and must be re-entered.

NOTE: If you associate a photo with this user (see "Acquire and Edit User Photo" on page 20 in section 9), that photo will show in the lower right corner of the User Data window.

6. Now update the access control network with the new information. Click on the UPDATE NET button on the tool bar (for details on the update process refer to “Update the Network” on page 35 in section 5

5.2.2 User Data – Spreadsheet Changes

When the EntraGuard feature is enabled in *Doors*, 5 new columns are added to the Setup Users Spreadsheet window to allow for data entry of necessary EntraGuard information. Leaving any of these fields blank may result in the EntraGuard unit not functioning properly. For more details see “User Data – Spreadsheet Method” on page 22 in section 4.

1. To enter user data through the spreadsheet method, click on the Setup ⇒ Users pull-down menu or click on the tool bar button. These two icons are added to the tool bar and the Setup Users spreadsheet window appears. If the spreadsheet is not visible, click on the tool bar button to ensure the Setup Users spreadsheet window is active (see Figure 10-54).

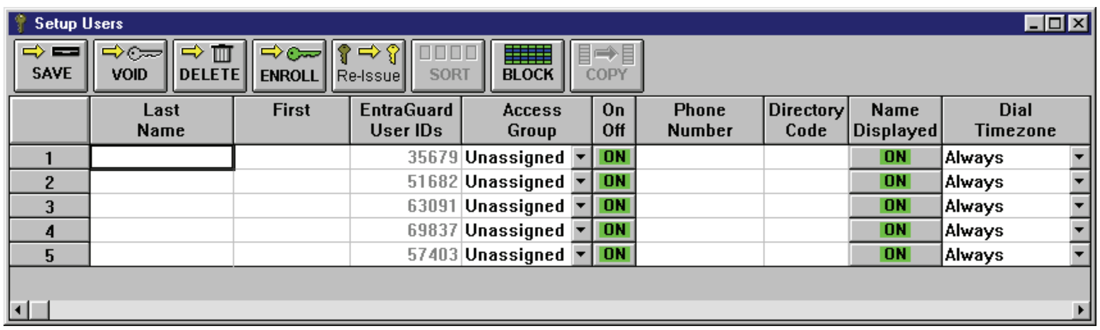


Figure 10-54: Setup Users Spreadsheet Window With New EntraGuard Columns

2. The following 5 fields are added for use with an EntraGuard unit. The rest of the fields may be filled in according to the instructions given in “Entering User Data – Spreadsheet Method” on page 22 in section 4.

   - EntraGuard User IDs – This number is automatically entered during enrollment and is the code tenants must use to enter through an EntraGuard controlled door.
   - Phone Number – This is the tenant’s home telephone number. The phone number cell may hold up to 15 characters. If it is necessary to use an area code for the EntraGuard controller to dial up the tenant’s phone, then that area code must be entered here (i.e. 1-800-555-3456).
   - Directory Code – This number is assigned by the operator as the number visitors must dial from the EntraGuard unit to dial up a tenant to request entry. Any number may be entered in this field, but is limited to the number of digits selected in “Select Directory Code and User ID Digits” on page 4 of this section.
   - Name Displayed – This cell allows a tenant’s name to appear on the EntraGuard’s LCD Directory List.
     1. To **disable** Name Displayed, locate the On/Off cell. It should be ON.
     2. Click on the cell; it changes to OFF.
     3. To **enable** Name Displayed, locate the On/Off cell. It should be OFF.
     4. Click on the cell; it changes to ON.

NOTE: Removing the tenant's name from the directory listing does not disable the ability of visitors to dial the tenant if they know the correct directory code.

- Dial Timezone – This number sets the hours a user will accept calls from visitors at the EntraGuard unit. To set up a time zone see "Setup Time Zones" on page 3 in section 3.

NOTE: All the columns may be sorted (see "Sorting Data" on page 29 in section 4). However, only the Directory Code, Phone Number, Dial Timezone, and Display Enabled columns may be block copied (see "Block Copying Data" on page 27 in section 4).

5. Click on the 

button to save these changes. If the User Data is not saved before clicking any other button or exiting the setup users window, the data entered is lost and must be re-entered.

6. You must update the access control network with the new information. Click on the 

button on the tool bar (for details on the update process refer to "Update the Network" on page 35 in section 5).

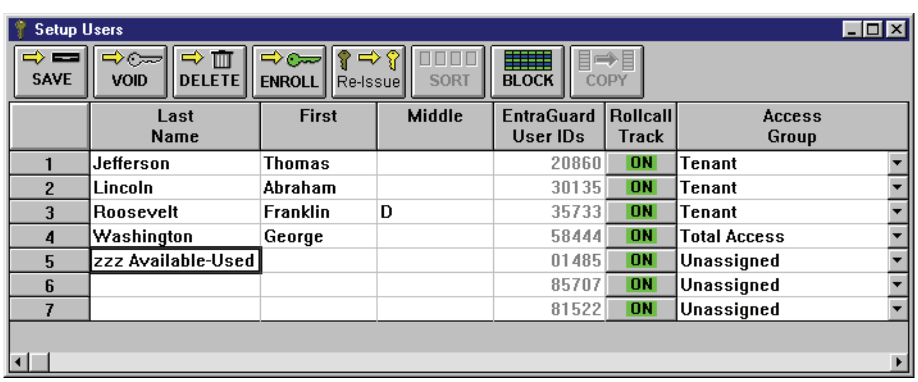
6.0 Void a User Changes

The void users feature allows an operator to remove a user from the access control database without removing the User ID from the database. That User ID can then be reassigned to a new user while maintaining the history of who has been assigned the User ID in the past.

6.1 Void a User Assigned a User ID Only

When a user who has been assigned only a User ID is voided (as shown in "Voiding a User – Dialog Box Method" on page 16 in section 4 or "Voiding a User – Dialog Box Method" on page 31 in section 4), the User ID remains in the database (just as the card does to do away with the need to re-enroll) but the Last Name column is changed to read "zzz Available - Used" (see Figure 10-55). This notifies the operator that although this User ID is now available for reissue, it is a User ID that has been assigned in the past.

NOTE: Reissue of User IDs brings with it possible problems that reissuing cards does not. Since all that is needed to gain access through an EntraGuard unit is a User ID, once a User ID is reissued, previous users who know that User ID can gain access. There is no way for the EntraGuard unit to tell between two different users entering the same User ID.



	Last Name	First	Middle	EntraGuard User IDs	Rollcall Track	Access Group
1	Jefferson	Thomas		20860	ON	Tenant
2	Lincoln	Abraham		30135	ON	Tenant
3	Roosevelt	Franklin	D	35733	ON	Tenant
4	Washington	George		58444	ON	Total Access
5	zzz Available-Used			01485	ON	Unassigned
6				85707	ON	Unassigned
7				81522	ON	Unassigned

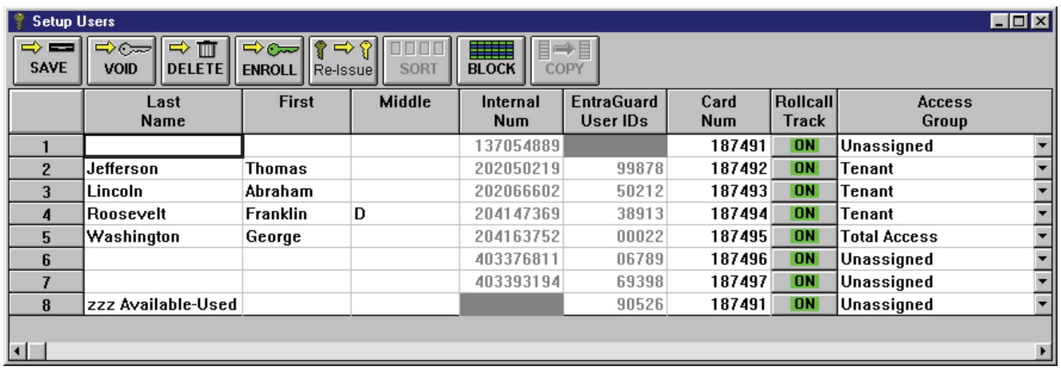
Figure 10-55: Voided User Assigned a User ID Only

The User ID remains in the user database and accomplishes three objectives.

- The User ID is available for reissue.
- The User ID will not be available for re-enrollment until it has first been deleted.
- As long as the User ID remains inactive (the ON/OFF column is OFF or the Activate User check box is blank), entry through an EntraGuard unit with that User ID will be denied.

6.2 Void a User Assigned a Card and a User ID

When a user who has been assigned a card and a User ID is voided (as shown in “Voiding a User – Dialog Box Method” on page 16 in section 4 or “Voiding a User – Dialog Box Method” on page 31 in section 4), the card and the User ID remain in the user database, each with their own row. The card is then available for reissue (a User ID may be added on later - see “Add User IDs to Previously Enrolled Cards” on page 23 of this section) and the User ID, while also available for reissue, is tagged in the Last Name column with “zzz Available - Used” (see Figure 10-56).



	Last Name	First	Middle	Internal Num	EntraGuard User IDs	Card Num	Rollcall Track	Access Group
1				137054889		187491	ON	Unassigned
2	Jefferson	Thomas		202050219	99878	187492	ON	Tenant
3	Lincoln	Abraham		202066602	50212	187493	ON	Tenant
4	Roosevelt	Franklin	D	204147369	38913	187494	ON	Tenant
5	Washington	George		204163752	00022	187495	ON	Total Access
6				403376811	06789	187496	ON	Unassigned
7				403393194	69398	187497	ON	Unassigned
8	zzz Available-Used				90526	187491	ON	Unassigned

Figure 10-56: Voided User Assigned a Card and a User ID

7.0 Identify an Unknown User ID

The *Doors* program is able to identify a User ID. In this example, the operator has a User ID number and wants to identify whose ID it is.

1. To identify an unknown User ID, click on the Reports ⇒ Find ID Card pull-down menu. The Find ID window appears (see Figure 10-57).
2. Click on the **By EntraGuard User ID** radio button.
3. Type the User ID number in the “User ID” cell.
4. Click on the 

button.
5. The user’s name and date of issue is displayed in the “Find ID Instructions and Results” field (see Figure 10-57).

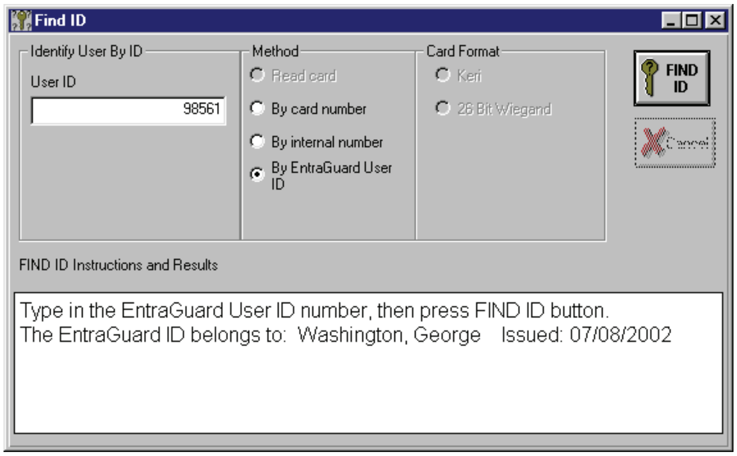


Figure 10-57: Find User ID Window With Results

8.0 Search For EntraGuard/Video-Related Events Using VideoTeleTrack

NOTE: Before searching for video-related events, make sure all events have been collected from the controllers.

1. To locate an EntraGuard event with any associated video clips using VideoTeleTrack, click on the  button, or the Reports ⇒ Searchable Events pull-down menu option (click on the VideoTeleTrack tab). The Event Reports window appears (see Figure 10-11).

NOTE: The information for locating EntraGuard/Video-related clips is the same no matter which option is used to open the report window.

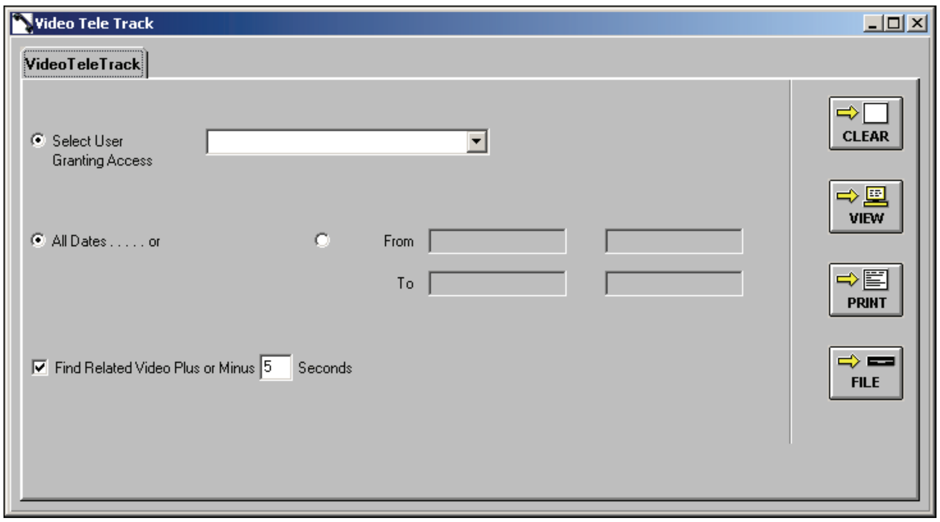


Figure 11: VideoTeleTrack Window

2. Verify there is a check mark in the “Find Related Video Plus or Minus 5 Seconds” check box. The default is set for 5 seconds before and after an event takes place, however this may be changed for up to 999 seconds before and after an event.

NOTE: If the check box is greyed out then the video feature has not been enabled (see “Enable Video in Doors” on page 3 in section 15).

3. Select the User and Dates to be searched, then click on the  button.
4. *Doors* will connect to the video server and search for events that match the search criteria.
5. If there was no data that meets the search criteria, an empty report warning window appears (see Figure 12).

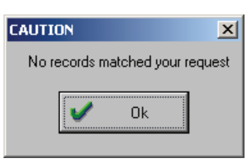


Figure 12: No Records Matched the Request Window

6. Click on the  button and modify the search criteria in the Quick Search window.
7. If the search was successful, a spreadsheet window appears (see Figure 13).

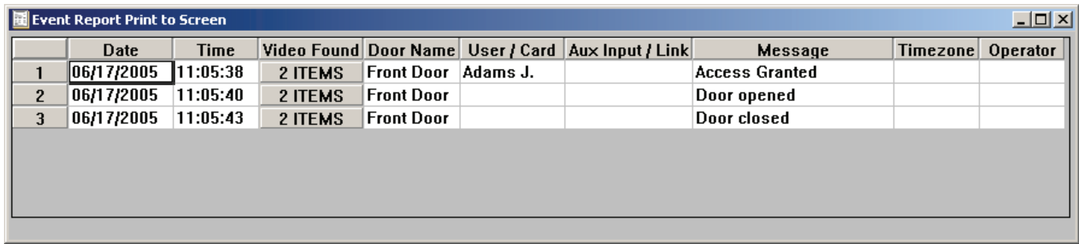


Figure 13: Event Report Print to Screen with Video Events Window

9.0 Disable EntraGuard

The EntraGuard feature can be disabled if necessary, removing all the EntraGuard related database fields. The EntraGuard ON check box is used to disable the EntraGuard feature (see Figure 10-1).

NOTE: Before disabling the EntraGuard feature, verify there is no check in the Remote Commands check box.

1. To disable the EntraGuard feature, click on the Setup ⇒ System pull-down menu or click on the  button on the tool bar, click on the **System Options** tab, then click on the 

button. The System Options window will change to reveal the options for setting the telephone entry options. The Systems Options window should look similar to the following window (see Figure 10-1).

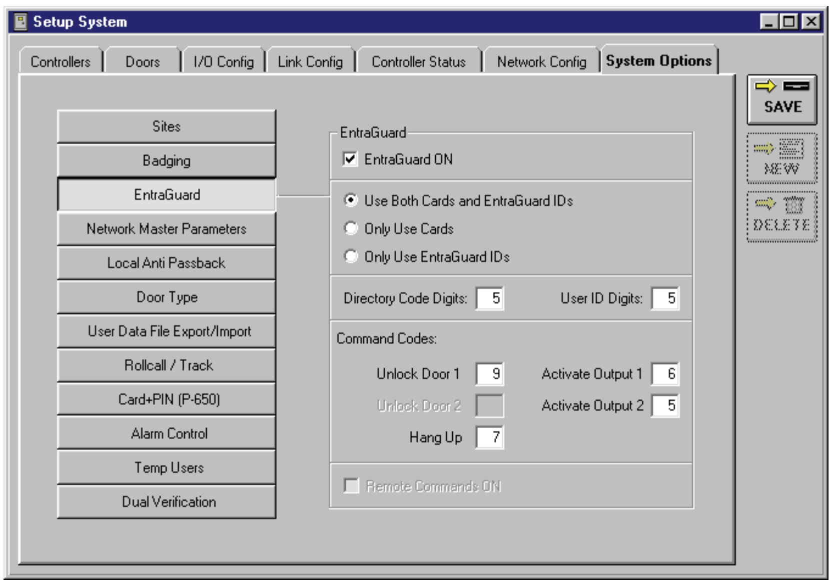


Figure 10-1: System Options Tab - EntraGuard Enabled

2. Click on the **EntraGuard ON** box. The check mark in the box disappears. Because the changes required to implement EntraGuard make major changes to the *Doors* program and its supporting databases, a confirmation window appears making this reminder (see Figure 10-2).

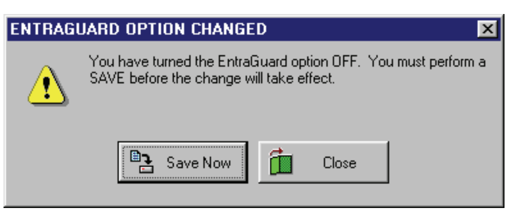


Figure 10-2: EntraGuard Option Changed - OFF

3. Click the 

button. All the EntraGuard related database fields are now disabled (see Figure 10-3).

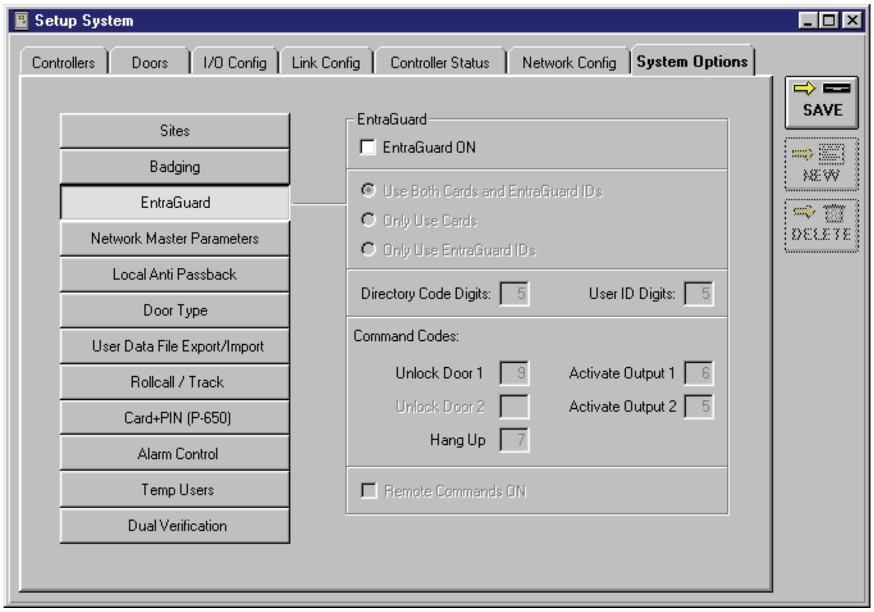


Figure 10-3: System Options Tab - EntraGuard Disabled

4. You must update the access control network with the new information. Click on the 

button on the tool bar (for details on the update process refer to “Update the Network” on page 35 in section 5).

10.0 *Doors* Features Not Used

The following features in *Doors*, although they may appear configurable, are not used with the EntraGuard Gold Telephone Entry Controller.

- Rollcall/Track - does not track use of the EntraGuard controller
- I/O Config - no configuration available
- I/O Link Config - no linking available
- First Person In - may enable, but has no effect

11.0 Troubleshooting EntraGuard Doors Features

Problem	Possible Cause	Corrective Action
Cardholder name not showing in directory list on EntraGuard LCD	1. User ID not enrolled as an EntraGuard ID. 2. User ID not turned ON. 3. No access group assigned. 4. No phone number listed. 5. Name displayed disabled.	1. Make sure the EntraGuard ID option is selected when enrolling User IDs. 2. Verify the ON/OFF cell is set to ON in the Setup Cards window. 3. Verify the Access Group does not say Unassigned. 4. Verify phone number cell contains correct phone number for cardholder. 5. Verify the Name Displayed cell is set to ON in the Setup Cards window.
User ID denied access	• User ID not enrolled as an EntraGuard ID • User ID not turned ON. • Not entering all numbers in the User ID.	• Make sure the EntraGuard ID option is selected when enrolling User IDs. • Verify on the Setup Cards spreadsheet that the ON/OFF cell is set to ON. • If the User ID number of digits (in the System Options window) is set for a specific number of digits (5 for example), then 5 digits must be entered (including any leading 0’s).
Telephone command does not perform function	• Pressing wrong telephone key for command.	• Verify the number assigned for the specific task on the System Options page is the correct number.
Unable to connect with cardholder’s phone	1. Wrong phone number entered. 2. Wrong time of day for Dial Timezone.	1. Verify phone numbered entered for cardholder is correct. 2. Check Dial Timezone to make sure it is set up correctly.

End of Section.

Section 11

User Data File Export/Import

User Data File Export/Import is integrated in the *Doors* program. User Data File Export/import allows a systems integration expert to export and/or import selected and limited user data from an external application. For more information on using the User Data File Export/Import feature see the User Data File Export/Import Application Note (P/N 01805-002).

Document Number 01914-011, Revision 5.2 – September, 2003

1.0 Enable User Data File Export/Import in *Doors*

The *Doors* User Data File Export/Import feature allows a systems integration expert to export then import selected and limited user data to/from an external application (such as Excel ™ or some similar spreadsheet or database program). Perform the following steps to enable the feature.

1. Click on the Setup ⇒ System pull-down menu or click on the  button on the tool bar, then click on the **System Options** tab. The System Options window appears. Click on the 

button to reveal the User Data File Export/Import field (see Figure 11-1).

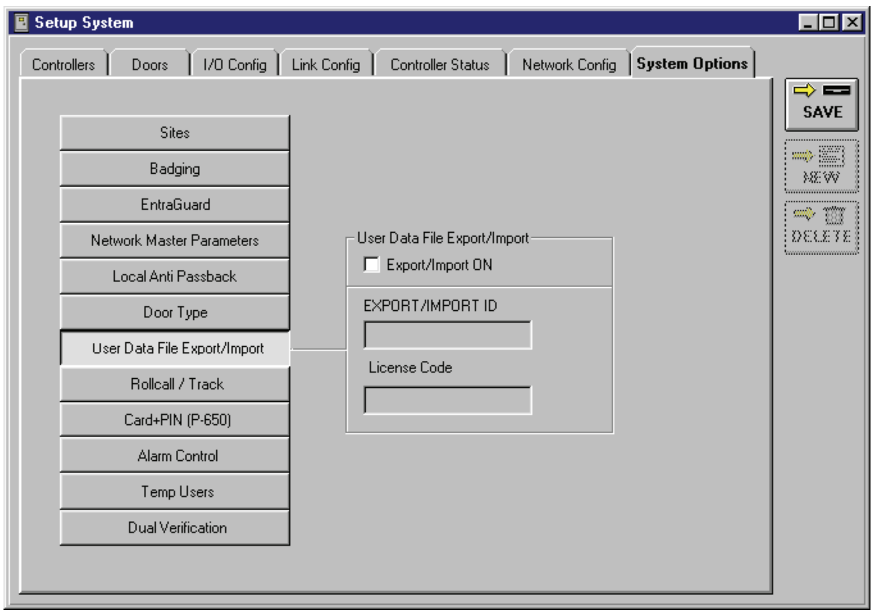


Figure 11-1: System Options Tab - User Data File Export/Import Disabled



NOTE: Mishandling the User Data File Export/Import feature may damage your user file database. Only allow a systems integration expert to use this feature. A License Code must be entered to activate the User Data File Export/Import feature. To receive a License Code you must call Keri Systems Customer Support at 1-800-260-5265 or 408-451-2520. They will need the EXPORT/ IMPORT ID number reported by the Doors program once the feature is enabled (see Figure 11-4 on page 4 of this section). With the EXPORT/IMPORT ID number, Customer Support will give you a corresponding License Code. The License Code is assigned to the specific computer used for User Data File Export/Import. User Data File Export/Import cannot be moved from one computer to another. If you attempt to do so, the License Code will be invalid.

2. To enable the User Data File Export/Import feature, click on the **Export/Import ON** check box. A check mark appears in the box. Because the changes required to implement the User Data File Export/Import feature make major changes to the *Doors* program and its supporting databases, a confirmation window appears (see Figure 11-2 on page 4 of this section).

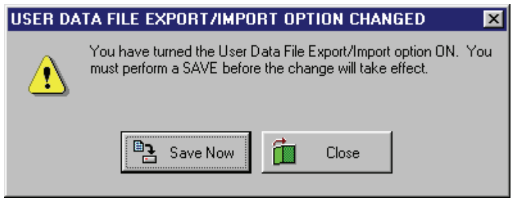


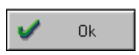
Figure 11-2: User Data File Export/Import Option Changed - ON

3. Click on the 

button and the User Data File Export/Import feature is enabled and a User Data File Export/Import Acknowledgement window appears (see Figure 11-3).



Figure 11-3: User Data File Export/Import Acknowledgment

4. Click on the 

button.
5. The EXPORT/IMPORT ID should now be visible inside the EXPORT/IMPORT ID box (see Figure 11-4). Have this number ready when you contact Keri Systems Customer Support to receive your License Code.
6. Once you have received your License Code from Keri Systems, enter the number in the "License Code" field.

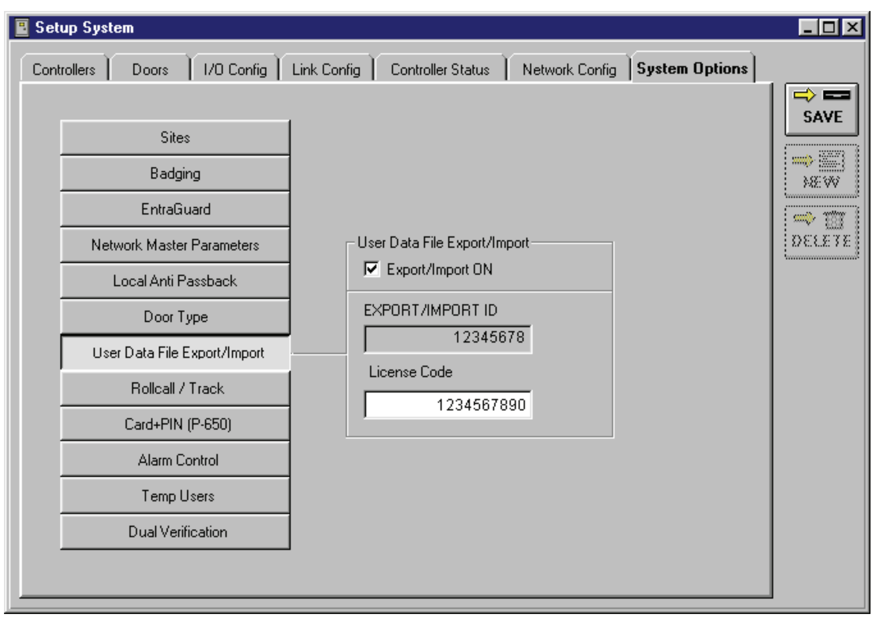


Figure 11-4: System Options Tab - User Data File Export/Import Enabled

7. Once you have entered the License Code, click on the  button.
8. If you have entered an incorrect License Code, a User Data File Export/Import Acknowledgement window appears (see Figure 11-3 on page 4 of this section). Click on the  button.
9. If you believe this message appeared in error, re-enter the License Code and click on the  button. If the Acknowledgment window reappears, contact Keri Systems Customer Support.
10. A number of database changes are now made to all the databases within the *Doors* program to support the User Data File Export/Import feature. When these changes are complete, the *Doors* program adds two new buttons to the System ⇒ Setup ⇒ Users spreadsheet,  and , to support User Data File Export/ Import. If a valid License Code was entered, you are now ready to use the User Data File Export/Import feature.

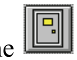
NOTE: If the Setup Users window is open, the new buttons will not appear until after you have closed, then re-opened the Setup Users window.

This page is intentionally left blank.

Section 12

Alarm Control

1.0 Enable Alarm Control

1. To enable Alarm Control, click on the Setup ⇒ System pull-down menu or click the  button on the tool bar. Click on the **System Options** tab followed by the 

button. The System Options window should look similar to Figure 12-1.

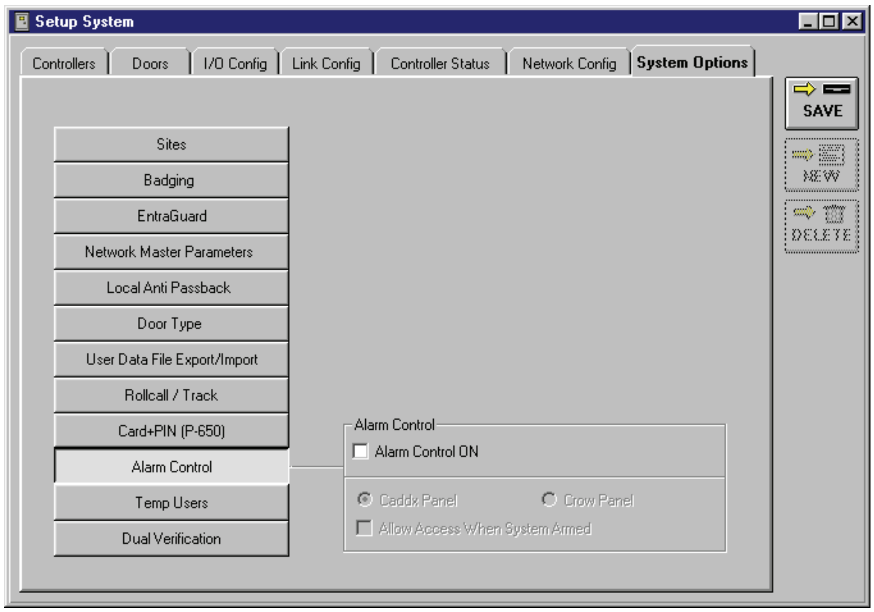


Figure 12-1: System Options Tab - Alarm Control Off

2. The default is for Alarm Control to be turned off.
3. Click in the check box beside the Alarm Control ON field. If a PXL-510 controller has not been detected as the master controller, an error message appears (see Figure 12-2).

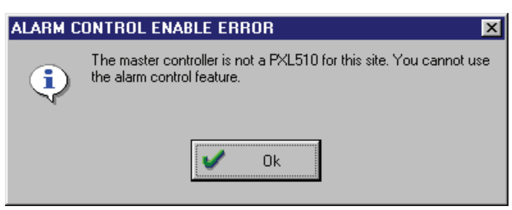


Figure 12-2: Alarm Control Enable Error

4. If a PXL-510 controller is set up as the master controller, perform an autoconfiguration (see "Autoconfiguration" on page 32 in section 2). Once the autoconfiguration is complete, return to click in the check box beside the Alarm Control ON field. If a PXL-510 was detected as the master controller during the autoconfiguration, a check mark appears in the check box and the following window appears (see Figure 12-3 on page 4).

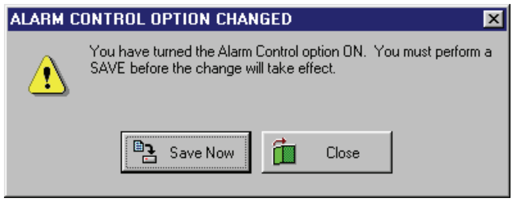
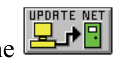


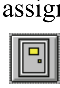
Figure 12-3: Alarm Control Option Changed Warning - ON

5. To enable Alarm Control, click on the  button. A “Saved Configuration” window flashes on the screen.
6. Select the type of panel to be used. The default is for Caddx panels. Crow Alarm Panels are available only in Australia. For all other areas of the world, the selection should be left at the default of Caddx.
7. To allow access even when the system is armed, click in the “Allow Access When System Armed” checkbox. The default is for this to not be selected.
8. Now update the access control network with the new information. Click on the  button on the tool bar (for details on the update process refer to “Update the Network” on page 35 in section 5).

2.0 Configure Reader in *Doors*

Once the Alarm Control feature has been enabled and the access control network has been updated, two columns (Alarm Control Reader Type and Allow Access While Alarm System Offline) are added to the **Doors** tab in the Setup System window (see Figure 12-4). These columns allow for specific configuration of the readers associated with the Alarm Control panel.

2.1 Assign Alarm Control Reader Type

1. To assign an Alarm Control Reader Type, click on the Setup ⇒ System pull-down menu or click the  button on the tool bar. Then click on the **Doors** tab. The Doors window appears (see Figure 12-4).

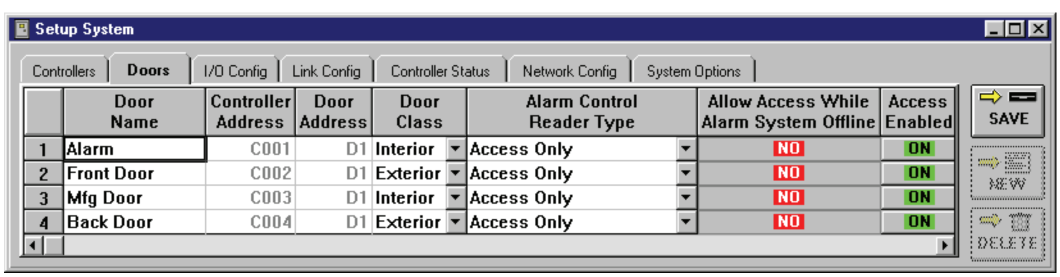


Figure 12-4: Setup System - Doors Tab

2. Scan down the door name and controller/door address columns and locate a door to be assigned an Alarm Control Reader Type.

3. Click on the drop-down arrow in the cell corresponding to the selected controller/door. The following options will appear:

- **Access Only** – This is used when no Alarm Control panel is in use at that particular reader.
- **Arm Only** – Presentation of a valid card will arm the alarm. A reader in this mode would not control access to a door nor disarm the alarm.
- **Disarm Only** – Presentation of a valid card will disarm the alarm. A reader in this mode would not control access to a door nor arm the alarm.
- **Arm/Disarm** – Presentation of a valid card will toggle the state of the Alarm Panel. If the Alarm Panel is armed, presentation of a valid card will disarm the alarm. If the Alarm Panel is disarmed, presentation of a valid card will arm the alarm. A reader in this mode will not control access to a door.
- **Access/Disarm** – Presentation of a valid card will disarm the alarm and grant access to the door.
- **Access/Arm** – Presentation of a valid card will grant access to the door while arming the alarm. **This option is not recommended because it has the potential to cause false alarms. However, it is available as an option for special applications.**

4. Click on the option pertaining to the selected controller/door.
5. Repeat steps 2 through 4 for each controller/door. The resulting window should look similar to Figure 12-5 on page 5.

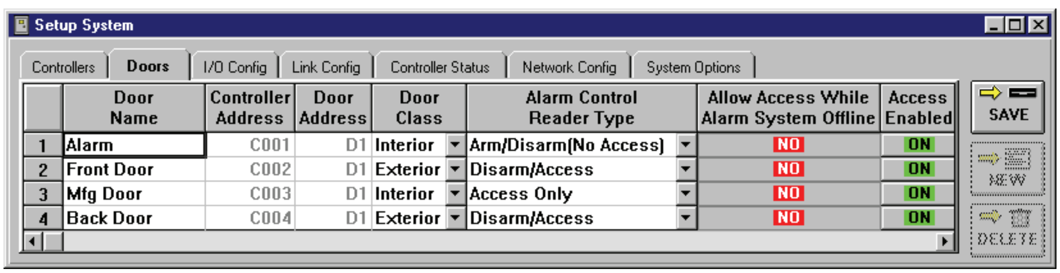


Figure 12-5: Setup System - Alarm Control Reader Type Set

2.2 Allow Access While Alarm System Offline

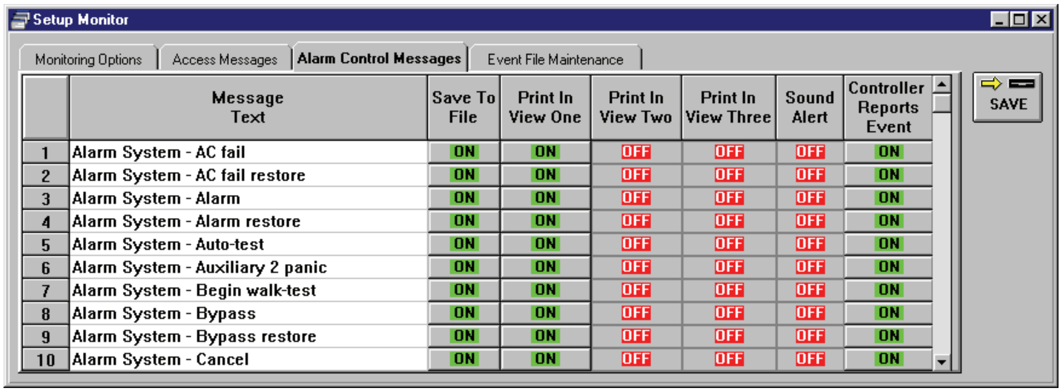
The Allow Access While Alarm System Offline column gives the operator the option to allow access through a controlled door even when the master controller has lost communication with the alarm control panel or, if the controller is a slave, with the master controller.

1. The default for the Allow Access column is set to NO.
2. To allow access while the alarm system is not in communication with the access control network, locate the NO cell corresponding to the controller/door that is to allow access. Click on the cell to toggle it to YES.
3. Once all the controllers/doors have been assigned an Alarm Control Reader Type and the Allow Access columns have been set, click on the SAVE button. If the changes are not saved before clicking any other button or exiting the System Setup window, the data entered is lost and must be re-entered.

NOTE: In order for a User to have the ability to arm/disarm the alarm control system, they must be set up to have access to the specific controller/door. For further instructions on how to give a User access to a specific controller/door, see the Doors Users Guide - Section 4: Setup Users (P/N 01914-100).

3.0 Alarm Control Message Text Strings

When the Alarm Control feature is enabled in Doors, an additional tab appears in the Setup Monitors window. There are 87 possible alarm control events that can be tracked. Each event is identified by a message text string that is a brief description of the event generated by the alarm panel when an event occurs. These strings can be edited by the operator to be more descriptive, making report viewing easier. There is a 40 character maximum for these text strings. For detailed information on ways to use the message text strings, refer to the *Doors* Users Guide (P/N 01914-100).



	Message Text	Save To File	Print In View One	Print In View Two	Print In View Three	Sound Alert	Controller Reports Event
1	Alarm System - AC fail	ON	ON	OFF	OFF	OFF	ON
2	Alarm System - AC fail restore	ON	ON	OFF	OFF	OFF	ON
3	Alarm System - Alarm	ON	ON	OFF	OFF	OFF	ON
4	Alarm System - Alarm restore	ON	ON	OFF	OFF	OFF	ON
5	Alarm System - Auto-test	ON	ON	OFF	OFF	OFF	ON
6	Alarm System - Auxiliary 2 panic	ON	ON	OFF	OFF	OFF	ON
7	Alarm System - Begin walk-test	ON	ON	OFF	OFF	OFF	ON
8	Alarm System - Bypass	ON	ON	OFF	OFF	OFF	ON
9	Alarm System - Bypass restore	ON	ON	OFF	OFF	OFF	ON
10	Alarm System - Cancel	ON	ON	OFF	OFF	OFF	ON

Figure 12-6: Alarm Control Message Text Strings

3.1 Alarm Control Message Text String Definitions

NOTE: 81 of the message text strings are generated by the alarm panel. For further information on these messages and what events generate them, refer to the NetworX documentation.

Alarm System ARM Request
Reported whenever a card is presented to a reader that has been set as an alarm arming reader.

Alarm System DISARM Request
Reported whenever a card is presented to a reader that has been set as an alarm disarming reader.

Alarm System Request Failed
Reported whenever an arm/disarm request has failed.

Master Communication Restored
Reported whenever communication between a master and slave controller is restored following a loss of communication.

Master Unable to Verify Slave Alarm Stat
Reported whenever access is denied on a slave or master because of a communication failure with the alarm panel.

PXL Slave Lost Communication with Master
Reported whenever communication between a master and slave controller occurs.

4.0 Disable Alarm Control in *Doors*

1. To disable Alarm Control, click in the Alarm Control ON check box. The check mark that was there disappears and the following window appears (see Figure 12-7).

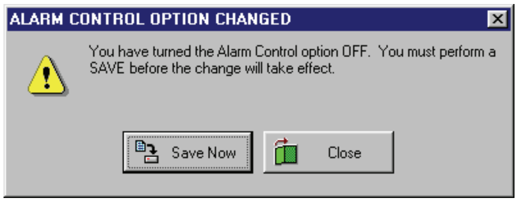


Figure 12-7: Alarm Control Option Changed Warning - OFF

2. Click the  button. A “Saved Configuration” window flashes on the screen.
3. Now click on the  button on the tool bar and update the access control network with the new information. For details on the update process refer to the *Doors* Users Guide (P/N 01914-100).

This page is intentionally left blank.

Section 13

Temp Users

1.0 Enable Temp Users

The Temp Users ON check box is used to enable the temp users feature (see Figure 13-1). The temp users feature allows an operator to set activation and expiration dates for the future. Once that pre-assigned date and time is reached, the controllers will either allow entry (if a pre-set activation date and time was set) or deny entry (if a pre-set expiration date and time has been set).

NOTE: The temp users feature only works with PXL-500 controllers. If you have a network with both PXL-500s and PXL-250s, the doors controlled by the PXL-250 will not recognize a pre-set activation or expiration date and will allow or deny entrance based only on whether the card has been turned on.

1. To enable the temp users feature, click on the Setup ⇒ System pull-down menu or click on the  button on the tool bar, then click on the **System Options** tab.
2. Click on the 

button. The System Options window will reveal the field for enabling temp users (see Figure 13-1).

NOTE: When the temp users feature is enabled, the user capacity drops from 65,535 possible users to 19,110 possible users.

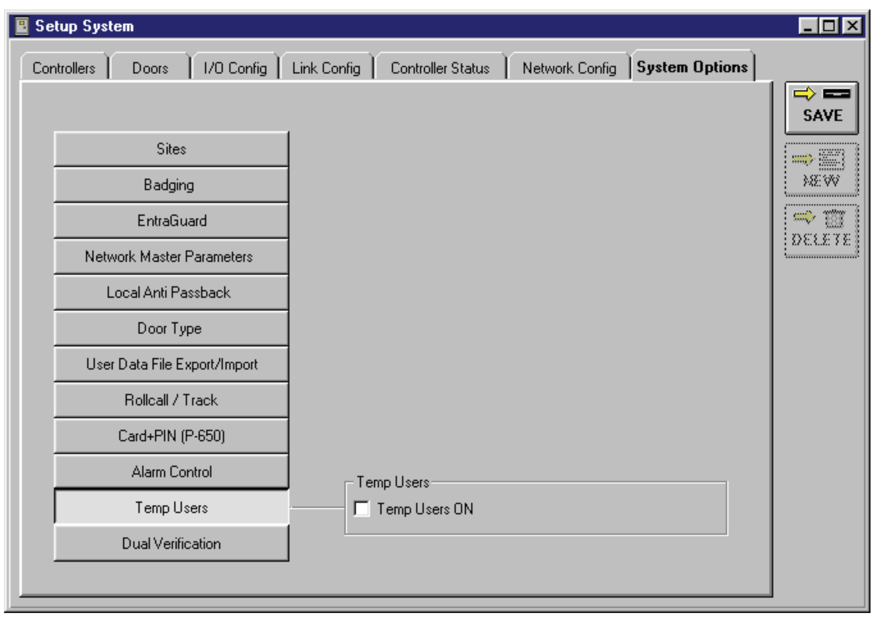


Figure 13-1: System Options Tab - Temp Users Disabled

3. Click on the **Temp Users ON** box. A check mark appears in the box. Because the changes required to implement the temp users feature make major changes to the *Doors* program and its supporting databases, a confirmation window appears (see Figure 13-2 on page 4 of this section).

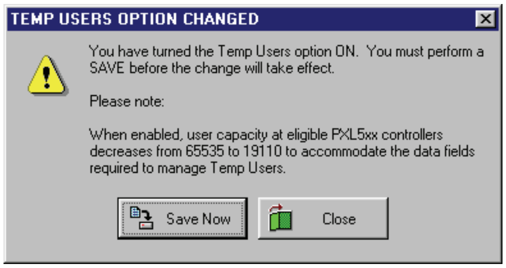


Figure 13-2: Temp Users Option Changed Window – ON

4. Click on the 

button and the conversion to Temp Users mode automatically occurs.

5. Now update the access control network with the new information. Click on the 

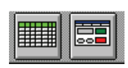
button on the tool bar (for details on the update process refer to “Update the Network” on page 35 in section 5).

2.0 Setup Users Changes

When the temp users feature is enabled changes are made to the Setup Users Spreadsheet and Setup Users Dialog Box. These changes allow for activation and expiration dates to be pre-set.

2.1 User Data – Dialog Box Changes

When the Temp Users feature is enabled in *Doors*, 4 new fields are added to the User Data tab to allow for data entry of pre-set activation and expiration dates. Leaving any of these fields blank will cause that user to be considered a standard user and all entry will be based on whether the card has been enabled or disabled. For more detail on the Dialog Box method of entering user data, see “User Data – Dialog Box Method” on page 13 in section 4.

1. To enter user data through the dialog box method, click on the Setup ⇒ Users pull-down menu or click on the  tool bar button. These two icons  are added to the tool bar and the Setup Users spreadsheet window appears.
2. Click on the  tool bar button to ensure the setup users dialog box window is active.
3. Click on the **User Data** tab. The User Data window appears (see Figure 13-3 on page 5 of this section).

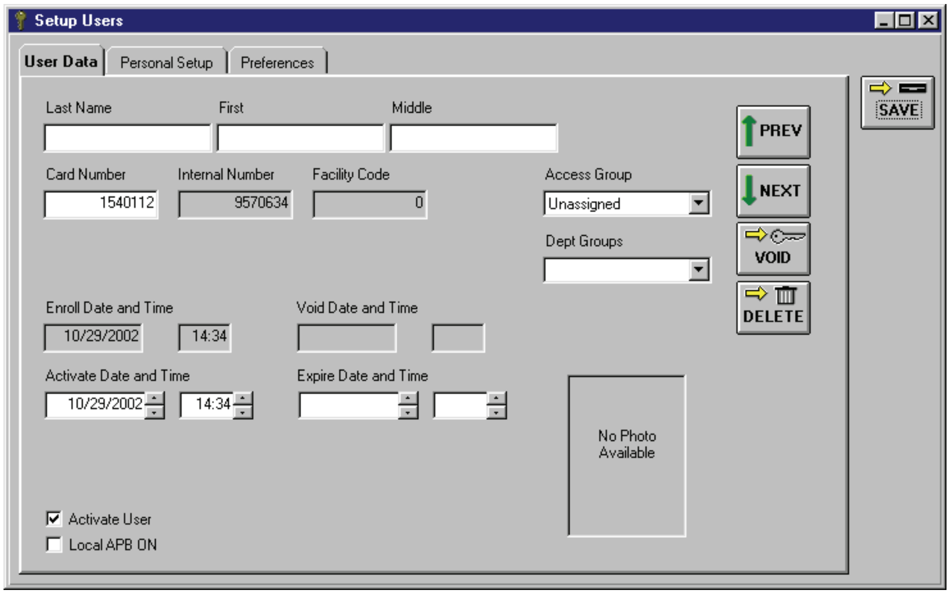


Figure 13-3: User Data Entry Window With New Temp Users Fields

NOTE: The Card Number, Internal Number, Facility Code, and Dept. Groups fields can be either visible or hidden depending on selections made on the Preferences tab. If one of these fields is not visible, click on the Preferences tab, and verify there is a check mark in the check box for the field you want displayed. If there is not a check mark in the check box, this field will be hidden on the User Data tab.

4. The following 4 fields are added for use with the Temp Cards feature. The rest of the fields may be filled in according to the instructions given in “Entering User Data – Dialog Box Method” on page 13 in section 4.

   - Activate Date and Time – When a date/time is entered in these fields and the card has been enabled, users will only be granted access once this date/time has passed. If this field is left blank, access is granted as soon as the card is enabled.
   - Expire Date and Time – When a date/time is entered in these fields and the card has been enabled, users will be granted access until this date/time is met. If this field is left blank, access is granted until the card is disabled.

5. Click on the 

button. If the user data is not saved before clicking any other button or exiting the User Data tab, the data entered is lost and must be re-entered.

6. Now update the access control network with the new information. Click on the 

button on the tool bar (for details on the update process refer to “Update the Network” on page 35 in section 5

2.2 User Data – Spreadsheet Changes

When the Temp Users feature is enabled in *Doors*, 4 new columns are added to the Setup Users Spreadsheet window to allow for data entry of pre-set activation and expiration dates. Leaving any of these fields blank will cause that user to be considered a standard user and all entry will be based on whether the card has been enabled or disabled. For more detail on the Spreadsheet method of entering user data, see“User Data – Spreadsheet Method” on page 22 in section 4.

1. To enter user data through the spreadsheet method, click on the Setup ⇒ Users pull-down menu or click on the  tool bar button. These two icons  are added to the tool bar and the Setup Users spreadsheet window appears. If the spreadsheet is not visible, click on the  tool bar button to ensure the Setup Users spreadsheet window is active (see Figure 13-4).

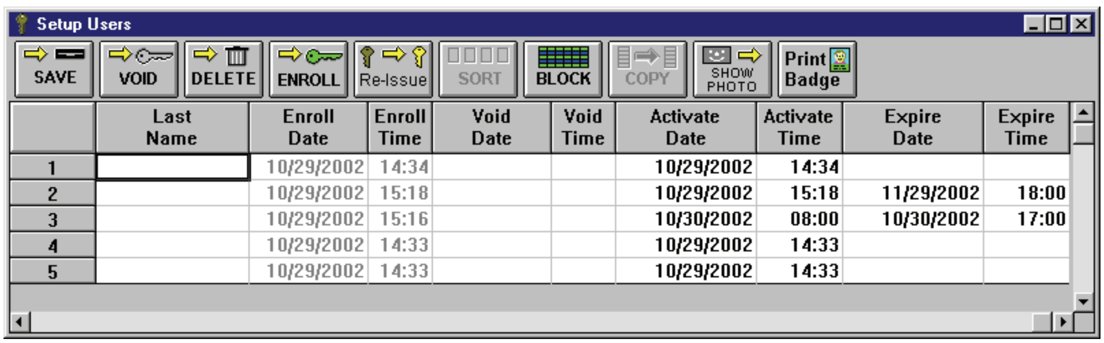


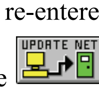
Figure 13-4: Setup Users Spreadsheet Window With New Temp Users Columns

2. The following 4 columns are added for use with the Temp Users feature. The rest of the fields may be filled in according to the instructions given in “Entering User Data – Spreadsheet Method” on page 22 in section 4.

   - Activate Date and Time – When a date/time is entered in these fields and the card has been enabled, users will only be granted access once this date/time has passed. If this field is left blank, access is granted as soon as the card is enabled.
   - Expire Date and Time – When a date/time is entered in these fields and the card has been enabled, users will be granted access until this date/time is met. If this field is left blank, access is granted until the card is disabled.

NOTE: All the columns may be sorted (see “Sorting Data” on page 29 in section 4). However, only the Directory Code, Phone Number, Dial Timezone, and Display Enabled columns may be block copied (see “Block Copying Data” on page 27 in section 4).

3. Click on the  button to save these changes. If the User Data is not saved before clicking any other button or exiting the setup users window, the data entered is lost and must be re-entered.

4. You must update the access control network with the new information. Click on the  button on the tool bar (for details on the update process refer to “Update the Network” on page 35 in section 5).

3.0 Disabling the Temp Users Feature

The temp users feature can be disabled if necessary, removing all the temp users related database fields.

The Temp Users ON check box is used to disable the temp users feature (see Figure 13-5). Perform the following steps to disable the temp users feature.

1. Click on the Setup ⇒ System pull-down menu or click on the  button on the tool bar, click on the **System Options** tab, then click on the 

button. The System Options window will change to reveal the temp users window (see Figure 13-5).

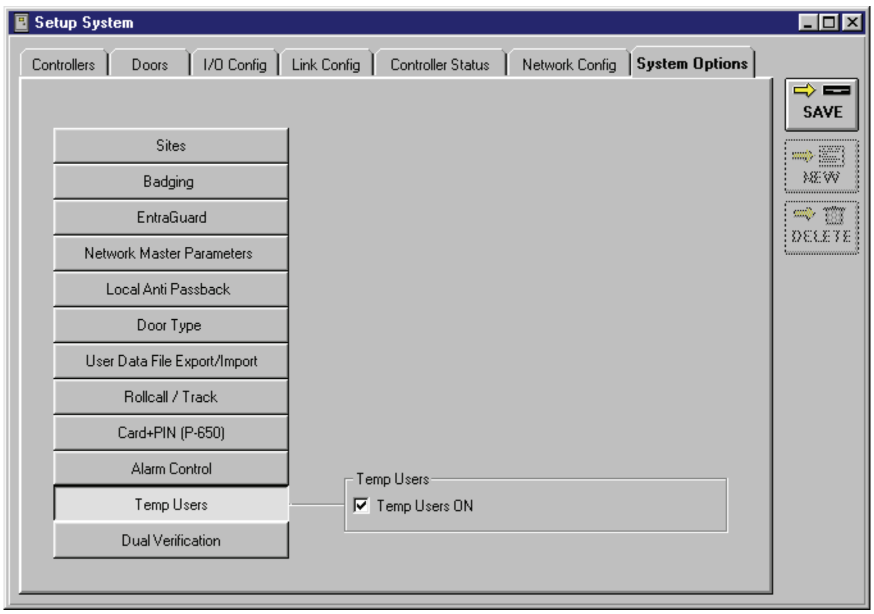


Figure 13-5: System Options Tab - Temp Users Enabled

2. Click on the **Temp Users ON** box. The check mark in the box disappears. Because the changes required to implement the temp users feature make major changes to the *Doors* program and its supporting databases, a confirmation window appears (see Figure 13-6).

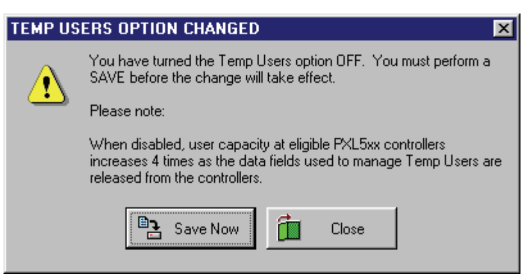


Figure 13-6: Temp Users Option Changed Window – OFF

3. Click the 

button. All the temp users related database fields are now removed and the system options window returns to its original state (see Figure 13-1 on page 3 of this section).

4. Now update the access control network with the new information. Click on the 

button on the tool bar (for details on the update process refer to "Update the Network" on page 35 in section 5).

Section 14

Dual Verification

Each person to be granted access to areas secured by Dual Verification will have assigned to them a Primary and Secondary ID. These may consist of cards and/or PINs (Personal Identification Numbers).

Document Number 01914-014, Revision 5.5 – September, 2003

1.0 Enable Dual Verification

The Dual Verification feature, when enabled on a controller, requires one or more credentials to gain access into a secure area. The first credential required is called the Primary ID with the second credential called the Secondary ID. For example, the Primary ID may be an access card with the Secondary ID a Personal Identification Number (PIN) used in connection with a keypad.

NOTE: The Dual Verification feature works with a Wiegand PXL-500/PXL-510 with proper firmware only. It is not necessary for the Wiegand controller to be the master controller, however the master controller must be a PXL-500/PXL-510.

1. To enable the dual verification feature, click on the Setup ⇒ System pull-down menu or click on the  button on the tool bar, then click on the **System Options** tab.
2. Click on the 

button. The System Options window will reveal the field for enabling dual verification (see Figure 14-1).

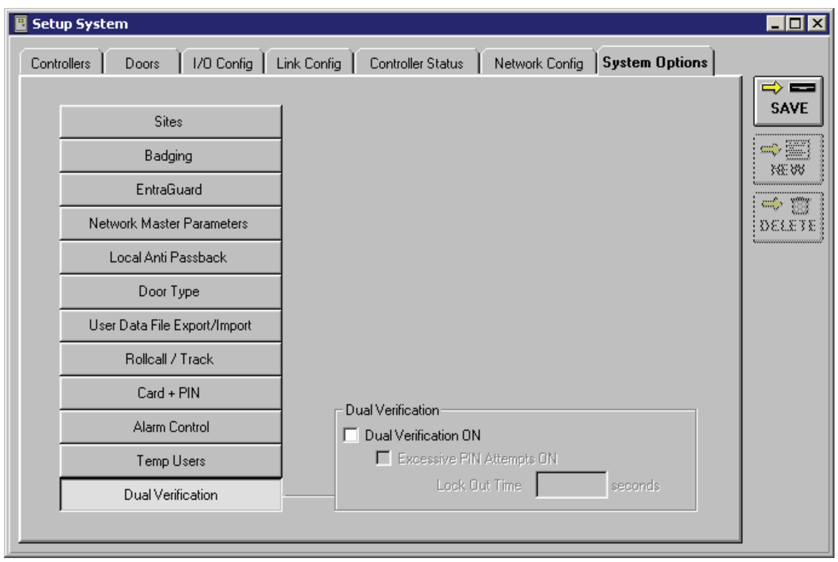


Figure 14-1: System Options Tab - Dual Verification Disabled

3. Click on the **Dual Verification ON** box. A check mark appears in the box. Because the changes required to implement dual verification make major changes to the *Doors* program and its supporting databases, a confirmation window appears (see Figure 14-2).

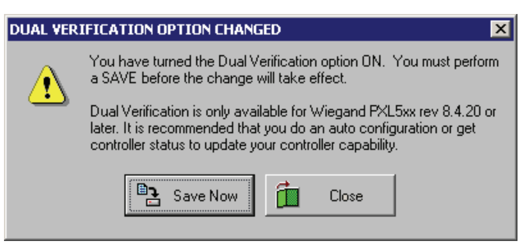
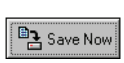


Figure 14-2: Dual Verification Option Changed Window – ON

4. Click on the 

button and the conversion to Dual Verification mode automatically occurs.

1.1 Excessive PIN Attempts

A user may have a maximum of 6 attempts to enter the proper Primary ID and Secondary ID before the reader or keypad gets locked out (not allowing any attempts) for a pre-set period of time.

1. To enable this feature, click on the **Excessive PIN Attempts ON** box. When there is a check in the box, the feature is enabled. To disable this field, click in the check box again and remove the check mark (this is the default value).

Once Excessive PIN Attempts has been enabled, a lock out time must be set. This is the period of time (in seconds) that the reader or keypad will lock out access following 6 failed attempts to enter a valid Primary and Secondary ID.

2. To set the lock out time, click in the Lock Out Time field and enter the number of seconds, ranging from 5-255 seconds, that the reader or keypad will remain in a lock out status
3. Click on the 

button to save these changes. If the Lock Out Time is not saved before clicking any other button or exiting the System Setup window, the data entered is lost and must be re-entered.
4. You must update the access control network with the new information. Click on the 

button on the tool bar (for details on the update process refer to "Update the Network" on page 35 in section 5).

2.0 Setup Secondary ID Required Time Zones

Once the Dual Verification feature has been enabled, time zones have an additional use. A Secondary ID Required Timezone must be applied to the Dual Verification reader/keypad defining the hours a Secondary ID is required to gain access through a door. The process to set up a Secondary ID Required Timezone is the same as setting up any time zone (see "Setup Time Zones" on page 3 in section 3).

NOTE: A Secondary ID Required Timezone is subject to the Access Timezone applied to the reader/keypad in Access Groups. If the Secondary ID Required Timezone is set for M-F 8am-8pm, but the reader/keypad's access Timezone is set for M-F 8am-6pm, access will be denied from 6pm-8pm. However, if the Secondary ID Required Timezone is set for M-F 8am-6pm and the reader/keypad's access Timezone is set for M-F 8am-8pm, access will be granted with only a Primary ID on M-F 6pm-8pm.

3.0 Setup Controllers/Doors

With the enabling of the Dual Verification feature, certain changes are made to the databases to allow for specific Dual Verification configuration.

3.1 Changes to Doors Configuration

Columns are added to the Doors tab once the Dual Verification feature has been enabled. The following is a list of those new columns.

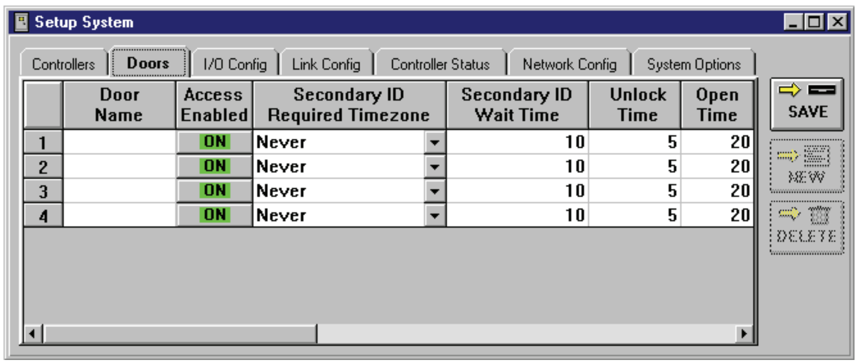


Figure 14-3: Setup System - Doors Tab Changes

<u>Secondary ID Required Timezone</u>
The Secondary ID Required Timezone defines the hours a Secondary ID is required to gain access through a Dual Verification controller.

<u>Secondary ID Wait Time</u>
The Secondary ID Wait Time is the amount of time (in seconds) that a Secondary reader or keypad will wait for input before requiring input of the Primary ID again.

NOTE: These new fields also appear on the Controller Status Tab.

4.0 Setup Users

Each person to be granted access to secured areas using the Dual Verification feature will need two credentials assigned to them. For the following enrollment examples, it is assumed the Primary ID will be a 26-bit Wiegand access card and the Secondary ID will be a PIN used on an Essex Keypad.

Through the Setup Users menu, an operator can enroll, void, and delete cards and PINs; assign cards and PINs to users; enter and edit user information, including personal data fields; and apply access groups to users. Once cards and PINs are enrolled, operators may use either the dialog box method or spreadsheet method for entering user data. The dialog box method (“User Data – Dialog Box Method” on page 13 in section 4) allows an operator to enter all user data through a series of “fill-in-the-blank” type windows. The spreadsheet method (see “User Data – Spreadsheet Method” on page 22 in section 4) allows an operator to enter all user data into a spreadsheet.

The following sections will instruct you on how to enroll users depending on the kind of system installed. Take a minute and determine what kind of access control system is in use.

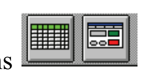
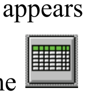
- Primary ID and Secondary ID - a new system
- Adding a Secondary ID to existing Primary ID system - when users have already been enrolled and a Dual Verification controller is being added to the system

4.1 Enrollment of Primary and Secondary IDs

If this is a new system (with no users enrolled) and a Dual Verification controller is on the system, each user will need to be assigned a Primary ID and a Secondary ID. They may be done at the same time or separately.

The following instructions are based on the assumption that the Primary ID will be an access card and the Secondary ID will be a Personal Identification Number (PIN) used with a keypad and that the enrollment of these credentials will take place at the same time.

4.1.1 Enrollment of Primary and Secondary IDs by Block Number Range

1. To enroll Primary and Secondary IDs by block number range, click on the Setup ⇒ Users pull-down menu or click on the  tool bar button. These two icons  are added to the tool bar and the Setup Users spreadsheet window appears (see Figure 14-4). If the setup users spreadsheet window is not visible, click on the  tool bar button.

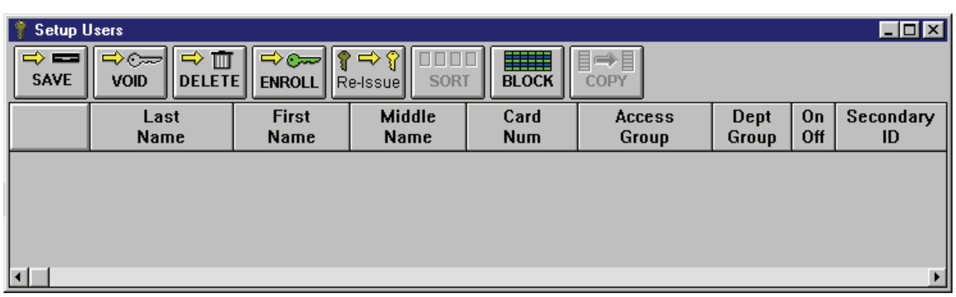
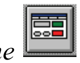


Figure 14-4: Setup Users Spreadsheet Window

NOTE: If the Setup Users window does not display the Secondary ID column, click on the  *button, select the Preferences tab, and verify the Show Secondary IDs check box has a check in it. If there is no check, click on the check box and a check will appear allowing the column to be displayed.*

2. Click on the  button. If the *Doors* program is not connected to the access control network, the program will automatically connect. The Enroll Cards window appears. Click on the  button. The Enroll Cards window is ready for block enrollment of Wiegand cards (see Figure 14-5).

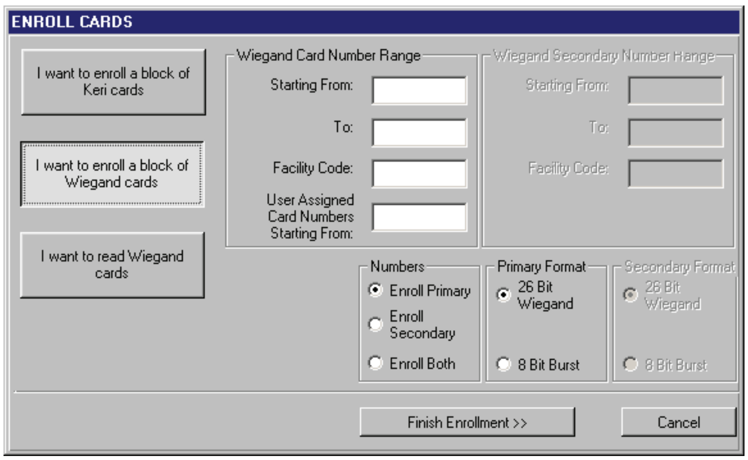


Figure 14-5: Enroll Cards - Block Enrollment

3. In the “Numbers” field, click on the Enroll Both radio button (see Figure 14-6).

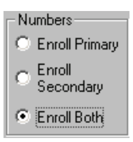


Figure 14-6: Enroll Cards - Numbers Field

4. In the “Primary Format” field, click on the radio button that corresponds to the type of format used for Primary ID (see Figure 14-7).

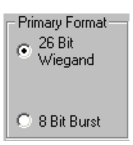


Figure 14-7: Enroll Cards - Primary Format Field

5. Once the Enroll Both radio button has been selected in the “Numbers” field, the “Secondary Format” and “Wiegand Secondary Number Range” fields become active. In the “Secondary Format” field, click on the radio button that corresponds to the type of format used for Secondary ID (see Figure 14-8 on page 8 of this section).



Figure 14-8: Enroll Cards - Secondary Format

6. Locate the “Wiegand Card Number Range” field. Click in the **Starting From** field. Enter the card number for the first card in the range of cards to be enrolled (the lowest number). For more information on how to locate the card number, see “Block Enrollment by Card Number Range” on page 3 in section 4.
7. Click in the **To** field. Enter the card number for the last card in the range of cards to be enrolled (the highest number).
8. Locate the **Facility Code** field and enter the facility code for the cards.

NOTE: For 26-bit Wiegand cards, facility codes may range from 0 to 255. The facility code is programmed into each card. To enroll cards, you ***must*** *know the facility code programmed into the card. If you do not know the facility code for the cards you are enrolling, please contact your card supplier for the facility code number* ***before*** *continuing the card enrollment process.*

NOTE: If you are block enrolling non-Keri Wiegand cards, be sure you know the actual internal card numbers programmed into the cards and verify the internal numbers are in consecutive order. Using incorrect numbers and non-consecutive cards invalidate the block enrollment process.

NOTE: If a facility code is not necessary, as is the case with an 8 Bit Burst keypad, the facility code field will not be visible.

9. The default for User Assigned Card Numbers is to copy the card number from the Wiegand Card Number Range field. If there is a need for user assigned card numbers that are different from the card number printed on the body of the card, click in the **User Assigned Card Numbers Starting From** field. Enter the user assigned number for the first card in the set. Numbers for the remaining cards will be assigned in ascending, sequential order from the first number. The Wiegand Card Number Range field should appear similar to Figure 14-9.

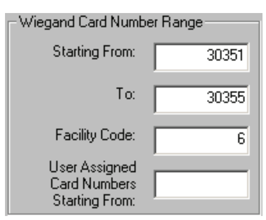


Figure 14-9: Enroll Cards - Wiegand Card Number Range

10. Locate the “Wiegand Secondary Number Range” field. Click in the **Starting From** field. Enter the PIN for the Secondary ID that will be associated with the first card enrolled. For 26 Bit Wiegand format, the number must be no more than 5 digits and cannot exceed 65,535 users. For 8 Bit Burst format the number must be no more than 4 digits and cannot exceed 999 users.
11. Click in the **To** field. Enter the PIN for the last PIN to be enrolled (the highest number).
12. If the Secondary ID requires a facility code, click in the **Facility Code** field and enter the facility code for the Secondary IDs. The “Wiegand Secondary Number Range” field should appear similar to Figure 14-10 on page 9 of this section.

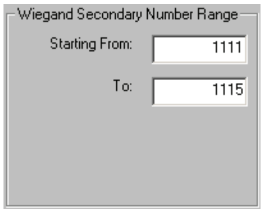


Figure 14-10: Enroll Cards - Wiegand Secondary Number Range

13. The resulting Enroll Cards window should look similar to Figure 14-11.

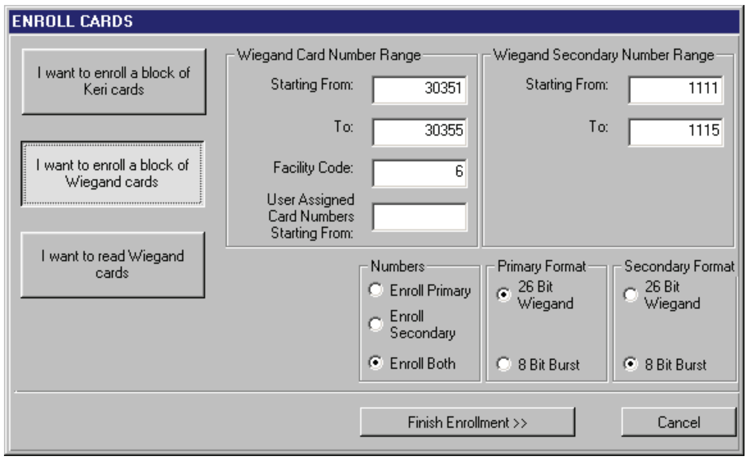
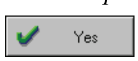
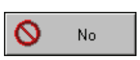


Figure 14-11: Enroll Cards - Ready For Enrollment

14. Click on the  button.

NOTE: If a large number of cards are being enrolled (greater than 5,000 cards at one time), it can take some time for the enrollment process to complete. A card quantity verification window appears (see Figure 14-12) to warn the operator of the time involved in enrolling a large number of cards at one time. Click on the  *button to continue with the enrollment. If the number of cards being enrolled is incorrect, or if you do not want to enroll such a large number of cards at one time, click on the*  *button.*

NOTE: Entering a large amount of cards by mistake (i.e 30,000) may be more than the host computer is able to handle.

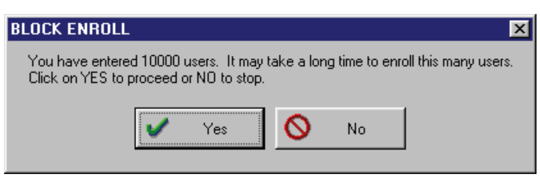
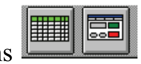


Figure 14-12: Block Enrollment Card Quantity Verification Window

15. Skip to "Verify Enrollment" on page 13 of this section.

4.1.2 Enrollment of Primary and Secondary IDs by Presenting to a Reader

NOTE: Enrollment by presenting to a reader for Dual Verification may be performed if the master controller is a Wiegand only. If the master controller is not a Wiegand, enrollment must be performed by block enrollment.

1. To enroll Primary and Secondary IDs by presenting to a reader, click on the Setup ⇒ Users pull-down menu or click on the  tool bar button. These two icons  are added to the tool bar and the Setup Users spreadsheet window appears (see Figure 14-13). If the setup users spreadsheet window is not visible, click on the  tool bar button.

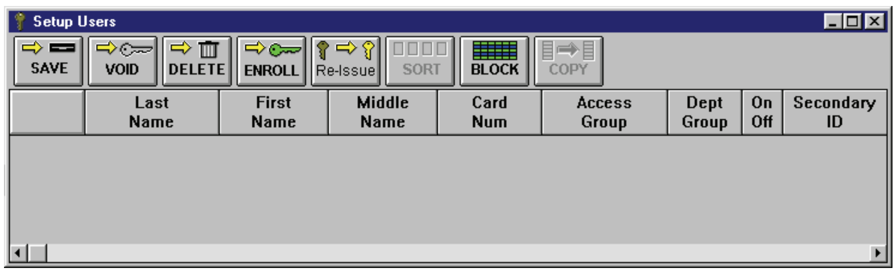
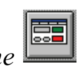
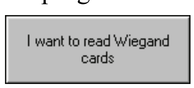


Figure 14-13: Setup Users Spreadsheet Window

NOTE: If the Setup Users window does not display the Secondary ID column, click on the  *button, select the Preferences tab, and verify the Show Secondary IDs check box has a check in it. If there is no check, click on the check box and a check will appear allowing the column to be displayed.*

2. Click on the  button. If the *Doors* program is not connected to the access control network, the program will automatically connect. The Enroll Cards window appears. Click on the  button. The Enroll Cards window is ready for enrollment of Wiegand cards by presenting to a reader (see Figure 14-14).

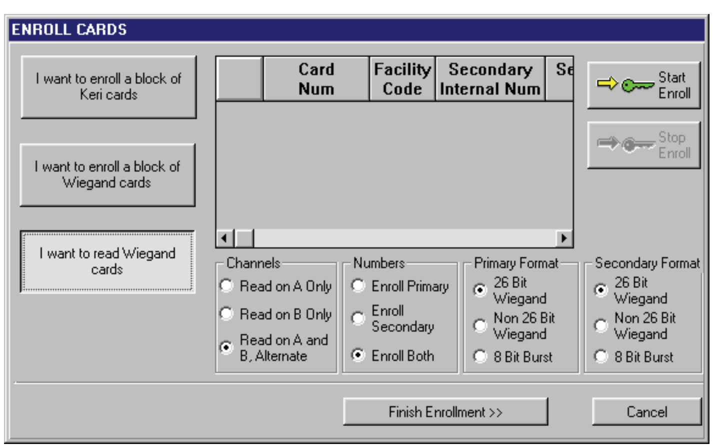


Figure 14-14: Enroll Cards - Presentation to a Reader

3. In the “Channels” field, select the reader or keypad channel to be used for enrollment. There are three options available; “A” reader, “B” reader, or both readers used alternately. For this example it is assumed that the “A” reader is a Wiegand card reader (and will be used as the Primary ID), and the “B” reader is a keypad (and will be used as the Secondary ID). See Figure 14-15.

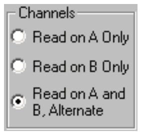


Figure 14-15: Enroll Cards - Channels Field

4. In the “Numbers” field, click on the Enroll Both radio button (see Figure 14-16).

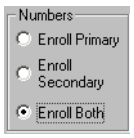


Figure 14-16: Enroll Cards - Numbers Field

5. In the “Primary Format” field, click on the radio button that corresponds to the format of the Primary ID (see Figure 14-17).

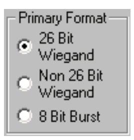


Figure 14-17: Enroll Cards - Primary Format Field

6. Once the Enroll Both radio button has been selected in the “Numbers” field, the “Secondary Format” field becomes active. In the “Secondary Format” field, click on the radio button that corresponds to the format of the Secondary ID (see Figure 14-18).

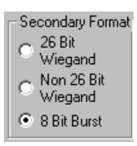


Figure 14-18: Enroll Cards - Secondary Format

7. Click on the 

button. If the *Doors* program is not connected to the access control network, the program will automatically connect.
8. The primary reader’s LED blinks green slowly to indicate it is ready for enrolling cards.

NOTE: The reader/controller is not available for any other use during the card enrollment process – any attempts to use a door associated with the master controller might disrupt the card enrollment process and will be denied until card enrollment is complete.

9. Present the first card to the enrollment reader. The reader will beep to indicate the card was read successfully and the card information will appear in the Enroll Cards window.

NOTE: If the Doors program is unable to enroll a card (because that card is faulty or has already been enrolled), the reader will provide one long beep and an error message window is displayed providing a brief description of the problem with the card being enrolled. Click the 

button to acknowledge the error message; then correct the problem and continue card enrollment. If there is no acknowledgement by the reader, after a card has been presented, the card may be of a format that is incompatible with the reader.

10. The Secondary ID keypad's LED blinks slowly to indicate it is ready for enrolling the Secondary ID. On an Essex Keypad, press the keys for the secondary ID (maximum of four digits) followed by the # key.
11. Return to the primary reader and present the next card. Once it is accepted, the secondary reader will be ready for enrollment of the Secondary ID.
12. Continue presenting cards and entering PINs alternating between the reader and keypad until all have been enrolled. When completed, the card enrollment window should look similar to Figure 14-19.

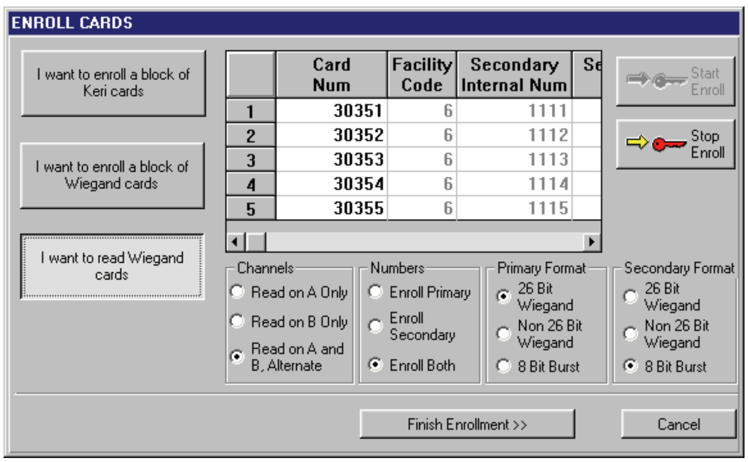


Figure 14-19: Enroll Cards - Presentation to a Reader Completed

13. Click on the 

button.
14. Continue on to “Verify Enrollment” on page 13 of this section.

4.1.2.1 Verify Enrollment

1. Once you have made your enrollment selections and clicked on the 

button, the Enroll New Users confirmation window will appear (see Figure 14-20).

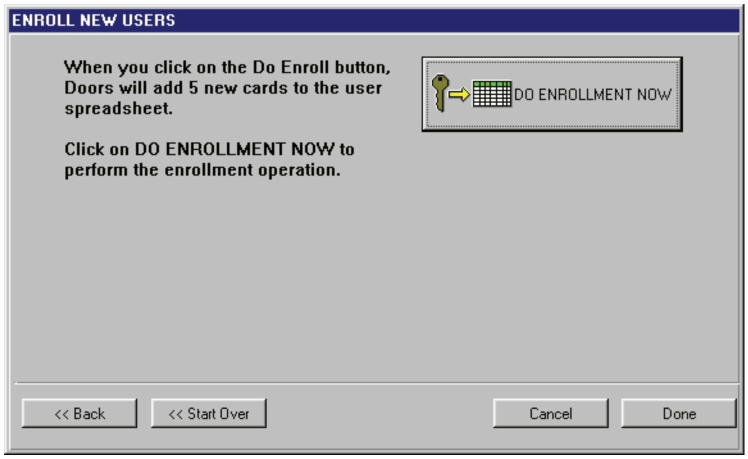


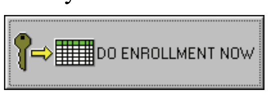
Figure 14-20: Enroll New Users Confirmation Window

2. The confirmation display shows the number of users you are about to enroll. Take a moment to verify this number is correct. If this number is incorrect, click on the 

button or the 

button to return to the Enroll Cards window to make changes.

NOTE: When using Dual Verification, the Enrollment Confirmation Window will not show the total number of credentials enrolled, but the total number of paired credentials. If you are enrolling 5 new users, each with two credentials to be used with Dual Verification, the Enrollment Confirmation Window will show 5 new enrollments, not 10.

3. Once you have verified all the information is correct on the confirmation display, click on the 

button. The credentials are enrolled and the enrollment results are displayed (see Figure 14-21).

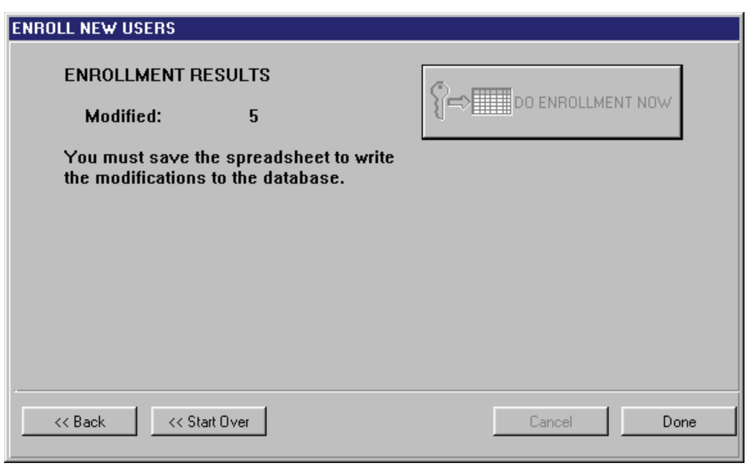


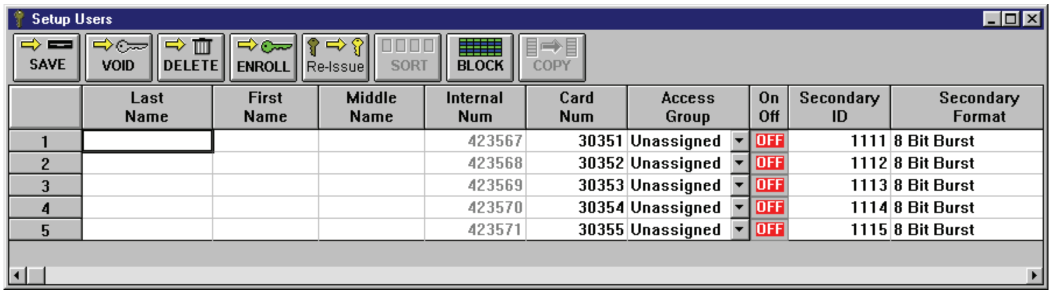
Figure 14-21: Enrollment Results Window

4. Carefully examine the information displayed under Enrollment Results. This field will alert you to the number of credentials that were successfully enrolled and if there were any errors or duplicate enrollments.

NOTE: If more than 100 credentials are being enrolled at one time, the enrollment results display will show the enrollment of credentials increase in increments of 100 until the database slots for all credentials being enrolled have been created.

5. Click on the 

button to close the Enroll New Users window. The setup users spreadsheet window now contains the newly enrolled users (see Figure 14-22).



	Last Name	First Name	Middle Name	Internal Num	Card Num	Access Group	On Off	Secondary ID	Secondary Format
1				423567	30351	Unassigned	OFF	1111	8 Bit Burst
2				423568	30352	Unassigned	OFF	1112	8 Bit Burst
3				423569	30353	Unassigned	OFF	1113	8 Bit Burst
4				423570	30354	Unassigned	OFF	1114	8 Bit Burst
5				423571	30355	Unassigned	OFF	1115	8 Bit Burst

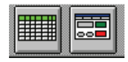
Figure 14-22: Setup Users Spreadsheet Window With Enrolled Cards and PINs

6. Click on the 

button to save the enrollment. If the enrollment information is not saved before clicking any other button or exiting the Setup Users window, the data entered is lost and must be re-entered.

4.1.3 Add Secondary ID to Previously Enrolled Primary IDs

In some cases Secondary IDs may need to be enrolled for users who already have cards/PINs assigned to them (for instance when an already existing system enables the Dual Verification feature).

1. To add Secondary IDs to users with previously enrolled cards/PINs, click on the Setup ⇒ Users pull-down menu or click on the  tool bar button. These two icons  are added to the tool bar and the Setup Users spreadsheet window appears (see Figure 14-23). If the setup users spreadsheet window is not visible, click on the  tool bar button.
2. The existing database should be visible with all previously enrolled users and their card information (see Figure 14-23).

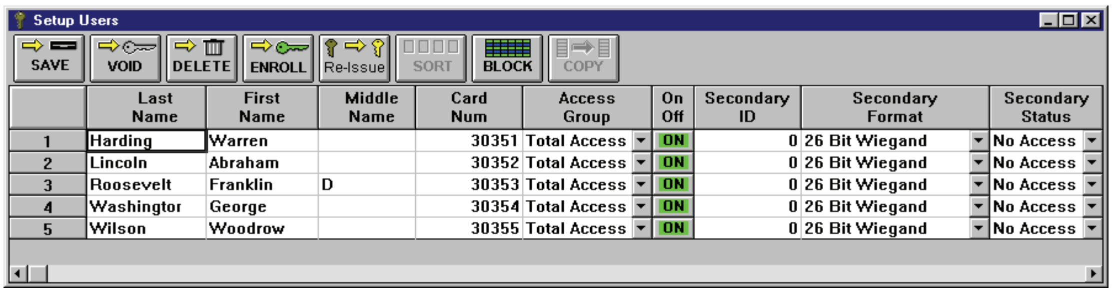


Figure 14-23: Setup Users Spreadsheet Window with Existing Card Users

NOTE: If the Setup Users window does not display the Secondary ID columns, make sure Dual Verification has been enabled. If the Secondary ID columns still do not appear, click on the  *button, select the Preferences tab, and verify the Secondary ID fields have check marks in the boxes. If there is no check, click on the check box and a check will appear allowing the column to be displayed.*

3. Click on the  button. If the *Doors* program is not connected to the access control network, the program will automatically connect. The Enroll Cards window appears (see Figure 14-24).

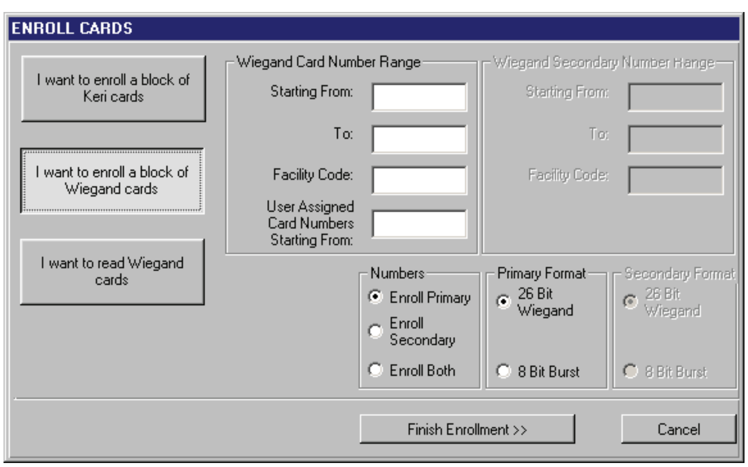


Figure 14-24: Enroll Cards Window

4. The process of filling out the Enroll Cards fields is the same either for enrolling by block number range or by presenting to a reader, except in the “Number” field. Select the radio button for **Enroll Secondary**.
5. In the “Secondary Format” field, select the format of the type of Secondary ID.
6. Once the block enrollment fields have been filled in or the credentials have been presented to a reader or keypad, click on the  button. The Add Secondary Numbers To All Users window will appear (see Figure 14-25).

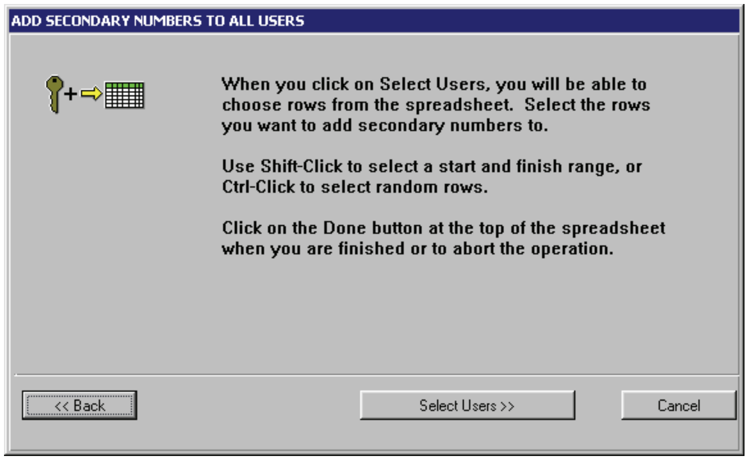


Figure 14-25: Add Secondary Numbers to All Users Window

7. Click on the  button. The Setup Users spreadsheet window will appear (see Figure 14-26). Any users already assigned a Primary and Secondary ID will not be visible.

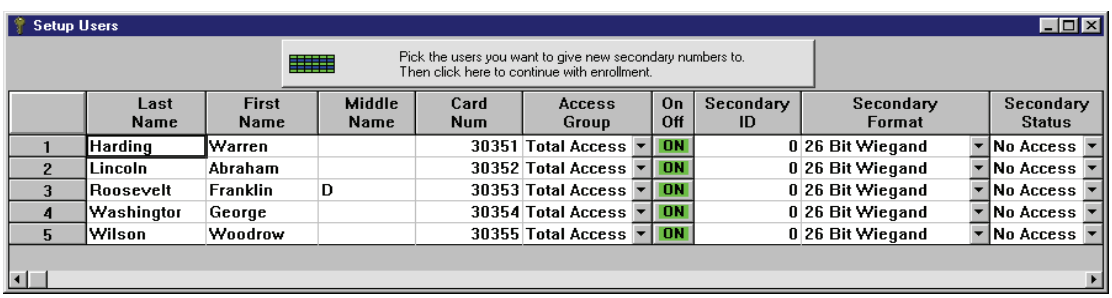


Figure 14-26: Setup Users - Select Users For Secondary ID Addition

8. Click on the users to be assigned a Secondary ID. There are three ways to select the users to which a Secondary ID should be assigned. Use the method you find easiest (see Figure 14-27 on page 17 of this section).

   - Click and hold on the row of the first user to be assigned a Secondary ID and drag the mouse down to the row of the last user.
   - Click on the row of the first user to be assigned a Secondary ID, hold the Shift key down, and click on the row of the last user.
   - Hold the Ctrl key down and one-at-a-time click on the rows of each user to be assigned a Secondary ID. This method is best used when the users are not in sequential order.

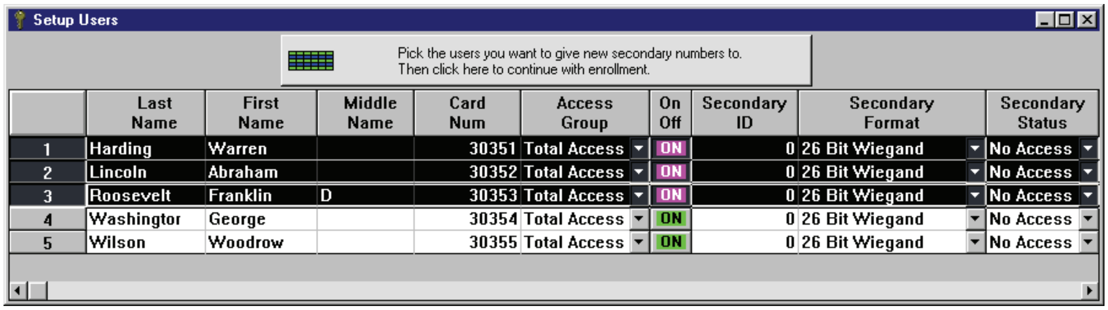
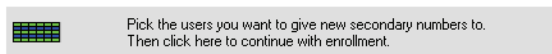


Figure 14-27: Setup Users - Selected Users for Secondary ID Addition

9. Once all the users to be assigned a Secondary ID have been selected, click on the 

button. The Enroll New Users window will appear (see Figure 14-28).

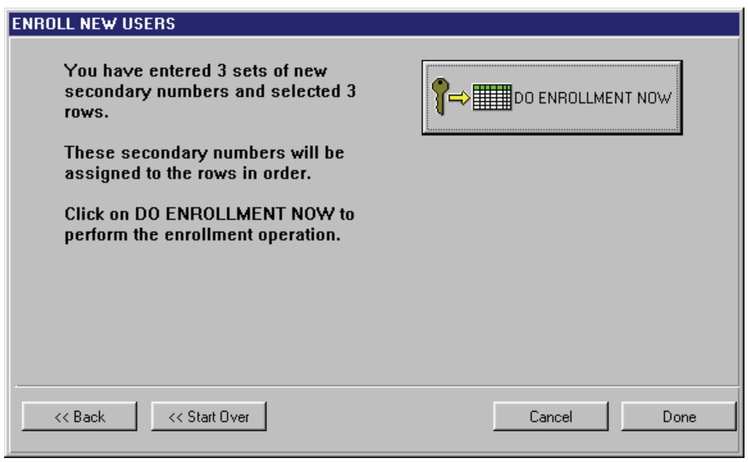
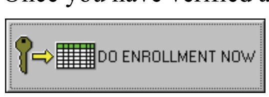


Figure 14-28: Enroll New Users Confirmation Window When Adding Secondary IDs

10. The confirmation display shows the number of Secondary IDs you are about to enroll. Take a moment to verify this number is correct. If this number is incorrect, click on the 

button to return to the Add Secondary Numbers To All Users window (see Figure 14-25 on page 16 of this section), or the 

button to return to the Enroll Cards window (see Figure 14-24 on page 15 of this section).
11. Once you have verified all the information is correct on the confirmation display, click on the 

button. The Secondary IDs are assigned to the selected spreadsheet rows and the enrollment results are displayed (see Figure 14-29 on page 18 of this section).

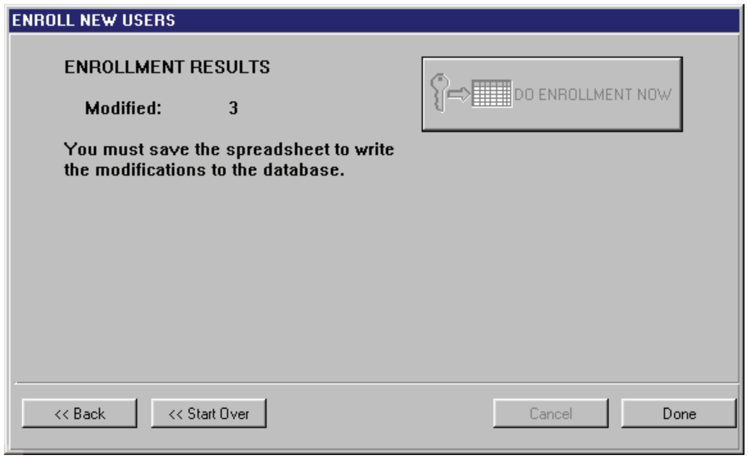
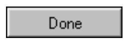


Figure 14-29: Enrollment Results Window

12. Carefully examine the information displayed under Enrollment Results.
13. Click on the  button to close the Enroll New Users window. The setup users spreadsheet window now contains the newly enrolled Secondary IDs (see Figure 14-30).

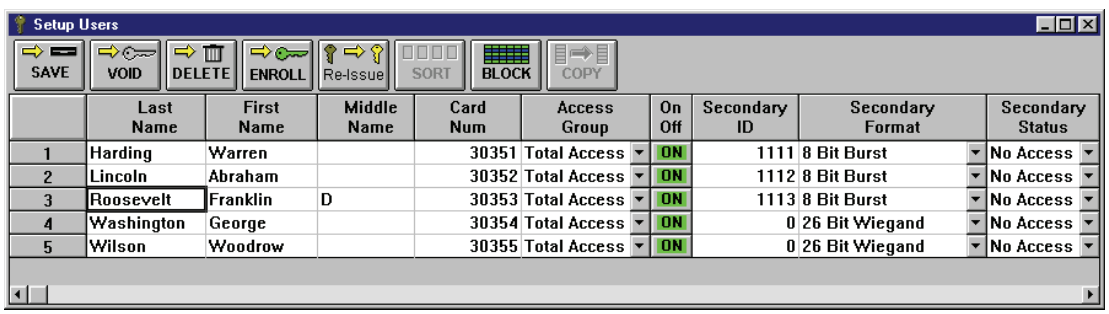


Figure 14-30: Setup Users Spreadsheet Window With Secondary IDs Added To Previous Users

14. Click on the  button to save the enrollment. If the enrollment information is not saved before clicking any other button or exiting the Setup Users window, the data entered is lost and must be re-entered.

4.2 Entering Dual Verification User Data

Once the Primary and Secondary IDs have been enrolled, data may be viewed, entered, or edited for all user data displayed in the spreadsheet.

4.2.1 User Data – Dialog Box Changes

When the Dual Verification feature is enabled in *Doors*, new fields are added to the User Data tab to allow for data entry of necessary Dual Verification information.

1. To enter user data through the dialog box method, click on the Setup ⇒ Users pull-down menu or click on the  tool bar button. These two icons  are added to the tool bar and the Setup Users spreadsheet window appears.
2. Click on the  tool bar button to ensure the setup users dialog box window is active.
3. Click on the **User Data** tab. The User Data window appears (see Figure 14-31).

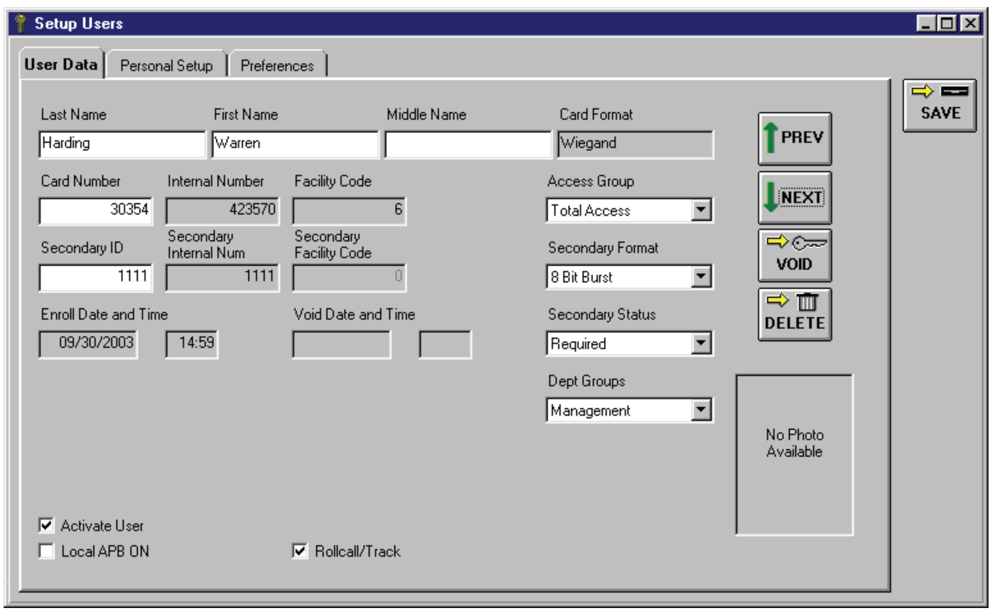


Figure 14-31: User Data Entry Window With New Dual Verification Fields

NOTE: Many of the fields can be either visible or hidden depending on selections made on the Preferences tab. Verify there is a check mark in the check box for the field you want displayed. If there is not check mark in the check box, this field will be hidden.

4. The following 5 fields are added for use with the Dual Verification feature. The rest of the fields may be filled in according to the instructions given in "Entering User Data – Dialog Box Method" on page 13 in section 4.

   - **Secondary ID** – This number is either a card number or PIN and is automatically entered during enrollment of the secondary ID. This field may be edited.
   - **Secondary Internal Number** – This number is automatically assigned during enrollment of the Secondary ID.
   - **Secondary Facility Code** – This is the facility code associated with the Secondary ID.
   - **Secondary Format** – This is the type of format used for Secondary ID.
   - **Secondary Status** – This determines when a user is required to provide a Secondary ID on readers/keypads where Dual Verification is in effect. Secondary Status is subject to the Secondary ID Required Timezone.
     Required - a Secondary ID is always required from this user in order to gain access.
     No Access - this user is not allowed access to Dual Verification readers/keypads.
     Exempt - this user may gain access simply by presenting their Primary ID. No Secondary ID is required.

5. Click on the 

button. If the user data is not saved before clicking any other button or exiting the User Data tab, the data entered is lost and must be re-entered.

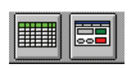
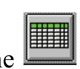
NOTE: If you associate a photo with this user (see "Acquire and Edit User Photo" on page 20 in section 9), that photo will show in the lower right corner of the User Data window.

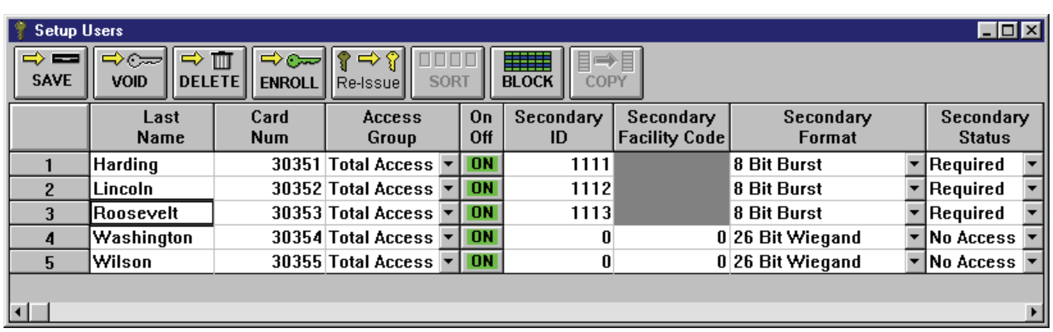
6. Now update the access control network with the new information. Click on the 

button on the tool bar (for details on the update process refer to "Update the Network" on page 35 in section 5

4.2.2 User Data – Spreadsheet Changes

When the Dual Verification feature is enabled in *Doors*, new columns are added to the Setup Users Spreadsheet window to allow for data entry of necessary Dual Verification information.

1. To enter user data through the spreadsheet method, click on the Setup ⇒ Users pull-down menu or click on the  tool bar button. These two icons  are added to the tool bar and the Setup Users spreadsheet window appears. If the spreadsheet is not visible, click on the  tool bar button to ensure the Setup Users spreadsheet window is active (see Figure 14-32).



	Last Name	Card Num	Access Group	On Off	Secondary ID	Secondary Facility Code	Secondary Format	Secondary Status
1	Harding	30351	Total Access	ON	1111		8 Bit Burst	Required
2	Lincoln	30352	Total Access	ON	1112		8 Bit Burst	Required
3	Roosevelt	30353	Total Access	ON	1113		8 Bit Burst	Required
4	Washington	30354	Total Access	ON	0	0	26 Bit Wiegand	No Access
5	Wilson	30355	Total Access	ON	0	0	26 Bit Wiegand	No Access

Figure 14-32: Setup Users Spreadsheet Window With New Dual Verification Columns

- **Secondary ID** – This number is either a card number or PIN and is automatically entered during enrollment of the secondary ID. This field may be edited.
- **Secondary Internal Number** – This number is automatically assigned during enrollment of the Secondary ID.
- **Secondary Facility Code** – This is the facility code associated with the Secondary ID.
- **Secondary Format** – This is the type of format used for Secondary ID.
- **Secondary Status** – This determines when a user is required to provide a Secondary ID on readers/keypads where Dual Verification is in effect. Secondary Status is subject to the Secondary ID Required Timezone.
  - **Required** - a Secondary ID is always required from this user in order to gain access.
  - **No Access** - this user is not allowed access to Dual Verification readers/keypads.
  - **Exempt** - this user may gain access simply by presenting their Primary ID. No Secondary ID is required.

NOTE: All the new columns may be sorted (see "Sorting Data" on page 29 in section 4). All new columns may also be block copied, except for the Secondary Internal Number column (see "Block Copying Data" on page 27 in section 4).

2. Click on the 

button to save these changes. If the User Data is not saved before clicking any other button or exiting the setup users window, the data entered is lost and must be re-entered.

3. You must update the access control network with the new information. Click on the 

button on the tool bar (for details on the update process refer to "Update the Network" on page 35 in section 5).

5.0 Disable the Dual Verification Feature

The Dual Verification ON check box is used to disable the dual verification feature. Perform the following steps to disable the dual verification feature.

1. Click on the Setup ⇒ System pull-down menu or click on the  button on the tool bar, click on the **System Options** tab, then click on the 

button. The System Options window will change to reveal the dual verification window (see Figure 14-33).

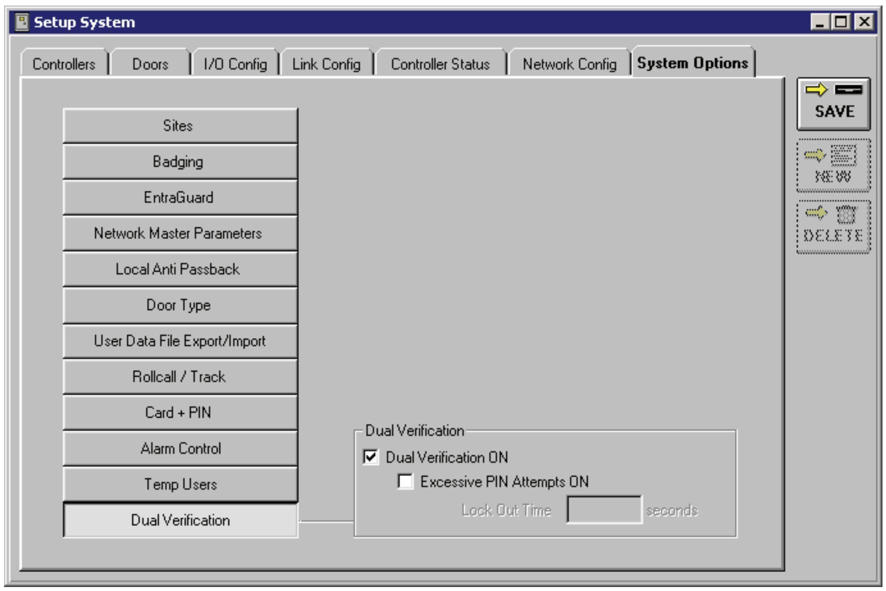


Figure 14-33: System Options Tab - Temp Users Enabled

2. Click on the **Dual Verification ON** box. The check mark in the box disappears. Because the changes required to implement the dual verification feature make major changes to the *Doors* program and its supporting databases, a confirmation window appears (see Figure 14-34).

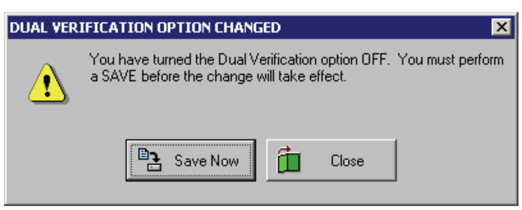
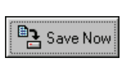


Figure 14-34: Dual Verification Option Changed Window – OFF

3. Click the 

button. All the dual verification related database fields are now removed and the system options window returns to its original state (see Figure 14-1 on page 3 of this section).

4. Now update the access control network with the new information. Click on the 

button on the tool bar (for details on the update process refer to “Update the Network” on page 35 in section 5).

Section 15

Visions Digital Video System

Keri's *Visions*™ Digital Video System combines *Doors* access control with digital video technology to provide stand-alone and integrated access plus CCTV solutions. The *Visions* product is comprised of a Digital Video Recorder (DVR) and *Visions* software, together known as the *Visions* Server. *Visions* Servers are available to work with 4, 8, 16, or 32 cameras, and can process up to 240 frames per second. Keri's *Visions* Digital Video System comes in either the one box solution (with the *Visions* Server and *Doors* software operating on a single PC), or a two box solution (with the *Visions* Server on one PC and the *Visions* Client software along with *Doors* software on a second PC).

Once cameras have been configured to coincide with doors, gates, or other input points on the *Doors* access control system, subsequent *Doors'* Quick Search reports will access the *Visions* Server application to find and list any access system events with associated video clips. Video clips are then available for playback on demand in a separate window.

The following documents need to be read and followed for proper operation of the *Visions* Digital Video System. All of these documents are available online at www.kerisys.com and on the Keri CD. The Visions Digital Video System Quick Start Guide (this document) has been included with your shipment.

- *Visions Server Setup and Users Guide* (P/N 01975-001)
- *Visions Client Setup and Users Guide* (P/N 01977-001)
- *Doors Users Guide* (P/N 01914-100)
- *Visions Digital Video System Quick Start Guide* (P/N 01974-001)

NOTE: For information on finding video clips related to Doors events, see the Visions Digital Video Quick Start Guide (P/N 01974-001).

Document Number 01914-015, Revision 5.9 – April, 2006

1.0 Enable Video in *Doors*

The *Doors* Video feature allows for the integration of the *Visions* Digital Video System and *Doors*. For detailed information on using Visions, see the Visions Quick Start Guide (P/N 01974-001). To enabled the video feature, perform the following steps:

1. Click on the Setup ⇒ System pull-down menu or click on the  button on the tool bar, then click on the **System Options** tab. The System Options window appears. Click on the 

button to reveal the Video field (see Figure 15-1).

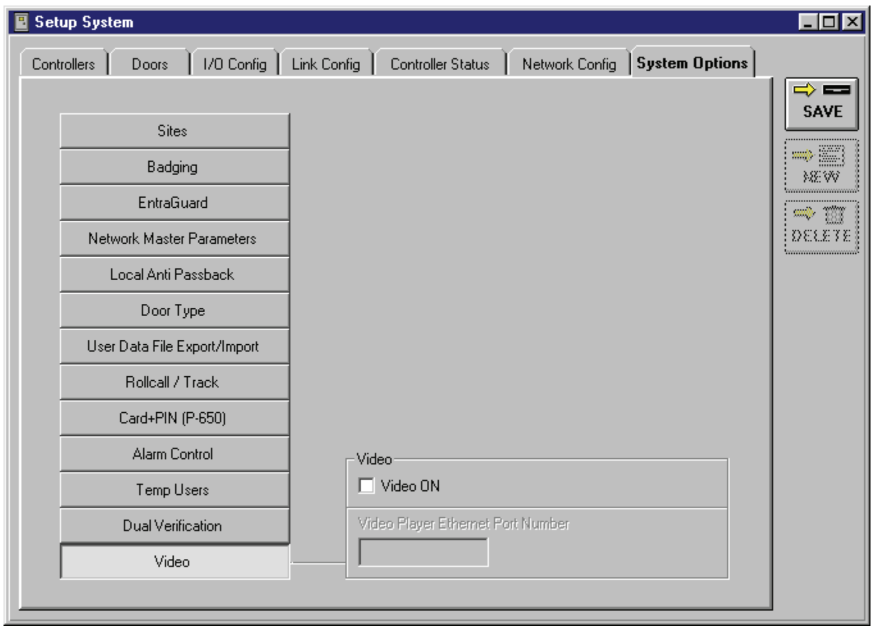


Figure 15-1: System Options Tab - Video Disabled

2. To enable the Video feature, click on the **Video ON** check box. A check mark appears in the box. Because the changes required to implement the Video feature make major changes to the *Doors* program and its supporting databases, a confirmation window appears (see Figure 15-2).

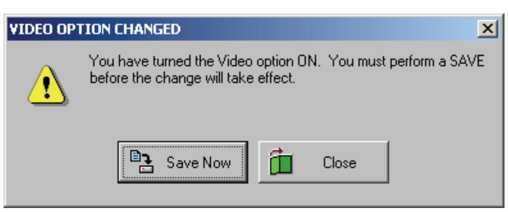
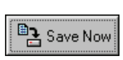


Figure 15-2: Video Option Changed - ON

3. Click on the 

button and the Video feature is enabled and a Video Player Ethernet Port Information window appears (see Figure 15-3 on page 4 of this section).

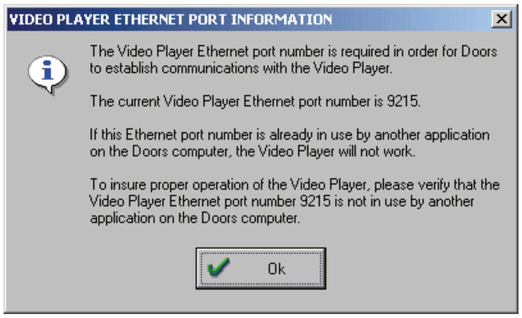


Figure 15-3: Video Player Ethernet Port Information

4. Click on the  button.
5. The port number 9215 should now be visible inside the Video Player Ethernet Port Number box (see Figure 15-4).

NOTE: It is highly unlikely that this port number is in use by another application. However, if Doors is unable to connect with the video server have the systems administrator check whether any application is using TCP port number 9215. Another port number may be assigned. Call Keri Technical Support for further details.

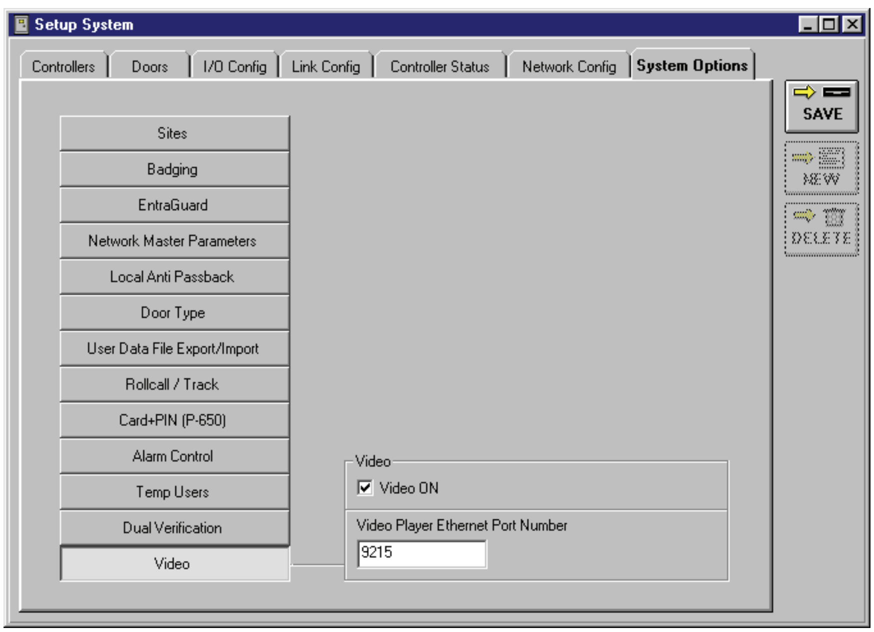


Figure 15-4: System Options Tab - Video Enabled with Assigned Port Number

6. Click on the  button.
7. A number of database changes are now made within the *Doors* program to support the Video feature. When these changes are complete, the *Doors* program starts the Keri Visions player.

NOTE: A  *button is added to the Windows Task Bar and the Visions CServer icon*  *is added to the Quick Launch area of the Task Bar.*

2.0 Configure Video Server Communications

NOTE: During the configuration process the video server should be running. However, if Doors and the Video Server are on a single PC, DO NOT log into the video server while configuring Doors.

Once the Video feature has been enabled and the access control network has been updated, *Doors* must be configured to communicate with the video server.

1. Click on the Setup ⇒ Video pull-down menu. The Setup Video window appears (see Figure 15-5).

NOTE: If Video does not show up as an option in the Setup pull-down menu, then the Video feature has not been enabled in Doors. For instructions on how to enable the Video feature, see “Enable Video in Doors” on page 3 of this section. If Video does show up as an option in the Setup pull-down menu, but is greyed out, check operator rights. For instructions on how to grant operator rights, see “Operator Rights” on page 48 of section 2.

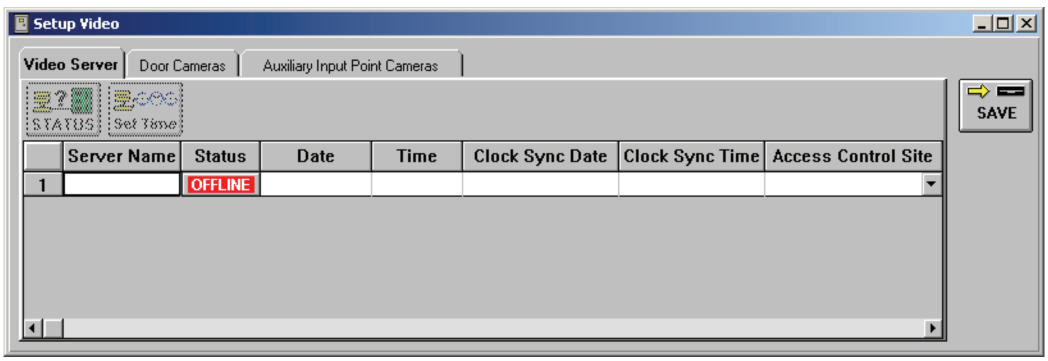


Figure 15-5: Video Server Tab

2.1 Video Server Tab

*NOTE: Some of the following fields are status only (marked by an *) and do not need any input from the operator. Those fields will remain blank until either the* 

or 

buttons are clicked.

Server Name
A descriptive text name for the video server. To assign a name to the video server, click on the “Server Name” cell and type a descriptive name for that server. The default for this field is blank.

Status*
Displays the status of the *Doors* connection to the video server.

Date*
Displays the date set on the video server PC.

Time*
Displays the time set on the video server PC clock.

Clock Sync Date*
Displays the date of the last sync of the access control network and the video server PC.

Clock Sync Time*

Displays the time of the last sync of the access control network clock and the video server PC clock.

Access Control Site

Lists all access control sites available for use with the video feature. Use the pull-down menu to select the access control site to be associated with the video server.

Server TCP/IP Address

Enter the TCP/IP address of the video server.

Server Ethernet Port

Displays TCP port on which the video server listens for Doors connection requests. The default is set for 7128 and should not be edited.

Server User ID

Enter a User ID that has been set up on the video server. For details on how to set up User IDs on the video server, refer to the *Visions Server Setup and Users Guide* (P/N 01975-001). The User ID is case sensitive and may be used by one program/operator at a time. It is recommended that a *Doors*-only User ID is set up.

Server Password

Enter the password that has been associated with the User ID entered. It must be the same as it was set up on the Video Server and is case sensitive.

Confirm Password

Enter the same password as in the previous field.

1. Click on the 

button to save these changes. If the Video Server information is not saved before clicking any other button or exiting the Setup Video window, the data entered is lost and must be re-entered. The clock synchronization automatially starts. Follow the steps beginning in "Synchronize Clocks" on page 7.
2. Once the clocks have been synchonized, the Video Server tab should then be similar to Figure 15-6.

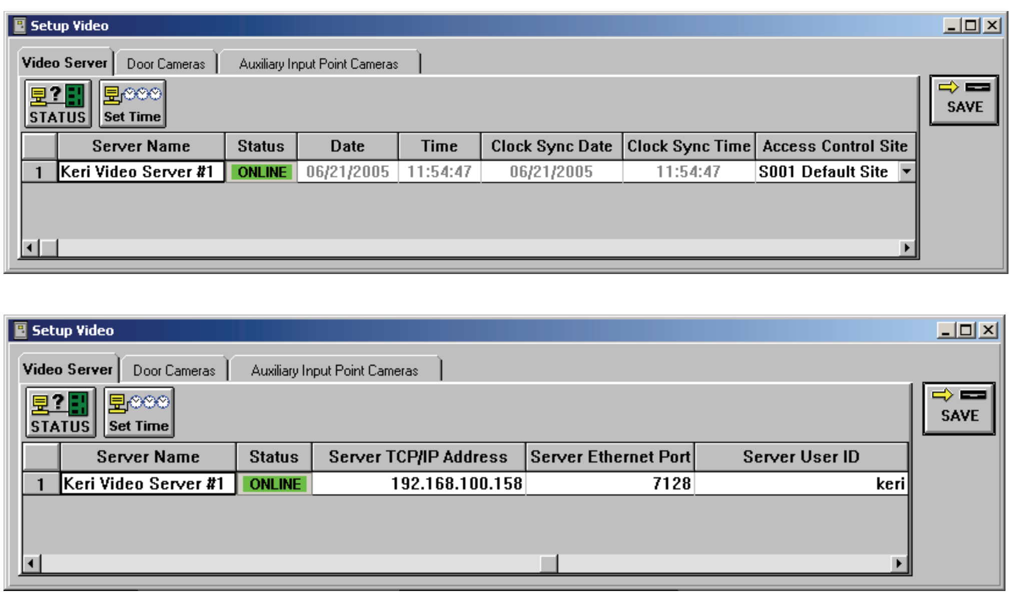


Figure 15-6: Video Server Tab

2.1.1 Synchronize Clocks

In order for the video clips to match up with *Doors* events, the clocks on the access control network and the video server must be synchronized. Once the Video Server information has been saved, a clock Synchronization window will appear (see Figure 15-7).

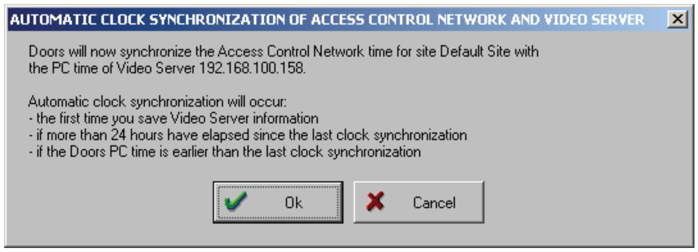


Figure 15-7: Automatic Clock Synchronization

1. Click on the  button to sync the clocks. A Two confirmation windows will appear (see Figure 15-8).

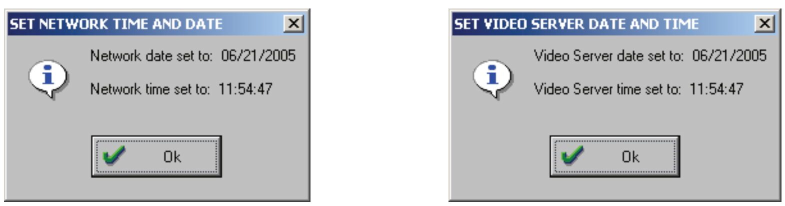
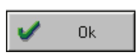


Figure 15-8: Network and Video Server Date and Time Synchronization Confirmation Windows

2. Click on the  button for each window to synchronize the clocks.

NOTE: The time sync will be based on the Doors PC clock and will not take into account different time zones.

NOTE: A synchronization reminder will appear every 24 hours, unless one of the following instances occur:

- *If the Doors PC clock gets set to a date and time prior to the saved clock sync date and time, a reminder to sync the clocks of the access control network and the video server will appear within 60 seconds.*
- *If the Doors PC clock is set to a date and time that is 24 hours or more after the saved clock sync date and time, a reminder to sync the clocks of the access control network and the video server will appear within 60 seconds.*
- *If Doors is in Monitor mode when a clock sync needs to take place, the clock sync will occur automatically without any input from the operator. If Doors has more than one site and a site other than the one associated with the video server is being monitored (Site #2), when the sync time arrives monitor mode will be suspended. Doors will temporarily disconnect from Site #2, connect to Site #1 (the one associated with the video server) and sync the clocks. Once that has completed, Doors will disconnect from Site #1, re-connect with Site #2 and resume monitoring. All this is done without any input from the operator, however messages will appear explaining what is taking place.*

3. To synchronize the clocks on demand, click on the  button and repeat steps 1 and 2.

2.2 Door Cameras Tab

Once the Video Server is set up, Cameras need to be assigned to specific physical doors. To assign door cameras, from the Setup ⇒ Video window, click on the Door Cameras Tab. The Door Cameras window appears (see Figure 15-9).

NOTE: Before beginning this section, assign camera names on the video server first. Once a camera has been assigned a name and assigned to specific doors, changing the camera name will require a new camer/door mapping.

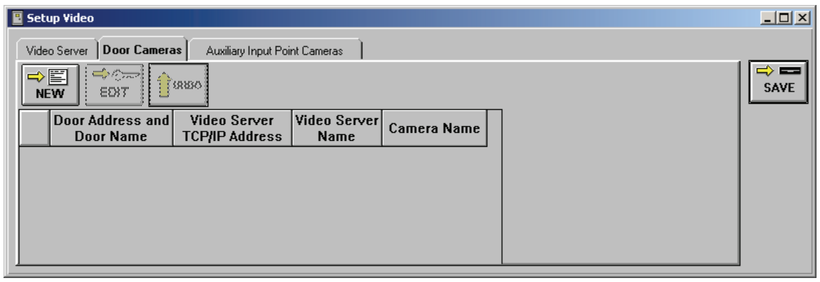


Figure 15-9: Door Cameras Tab

1. Click on the 

button. A new blank row appears.

Door Address and Door Name
From the pull-down list, select the physical door to be assigned a camera.

Video Server TCP/IP Address
The TCP/IP address of the video server is automatically entered.

Video Server Name
The Video Server Name that was entered during the Setup Video Server process appears here.

Camera Name
From the pull-down list, select the camera to be assigned to the door in the first column.

NOTE: More than one camera may be assigned to each door and more than one door may be assigned to each camera. It is all dependent on where the cameras are pointed.

2. Click on the 

button to save each row. Repeat the process for as many cameras/door combinations there are. If the information is not saved before clicking any other button or exiting the Setup Video window, the data entered is lost and must be re-entered.
   - To make changes to a row that has already been saved, click on the row that needs changed and then click on the 

button. Make the necessary changes and click on the 

button.
   - To remove a row before it has been saved, click on the row to be removed and then click on the 

button.
   - To remove a row after it has been saved, click on the row to be removed and then click on the 

button.

3. The finished window may appear similar to Figure 15-10.

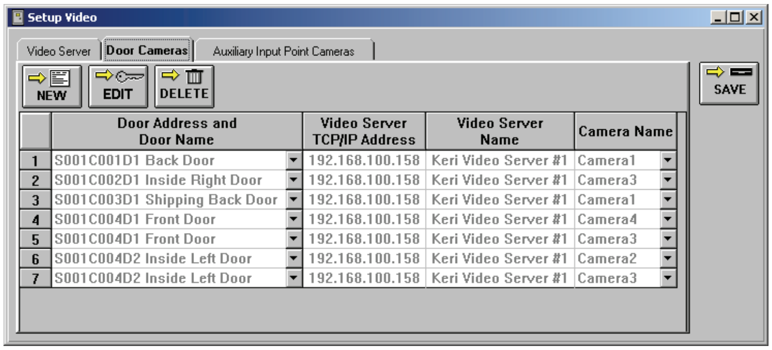


Figure 15-10: Door Cameras Tab with Doors and Cameras Assigned

NOTE: If a camera name has been changed, DO NOT delete the Door Camera Tab setup. Add a new row for the new camera name. If the old camera setup is deleted, Doors will not be able to find any video-related events that took place prior to the camera name change.

2.3 Auxiliary Input Point Cameras

For those using auxiliary inputs in Doors, cameras may be assigned to begin filming when specific inputs occur. To assign cameras to specific auxiliary inputs start from the Setup ⇒ Video window. Click on the Auxiliary Input Point Cameras Tab and the window appears (see Figure 15-11).

NOTE: Before beginning this section, assign camera names on the video server first. Once a camera has been assigned a name and assigned to specific inputs, changing the camera name will require a new camera/input mapping.

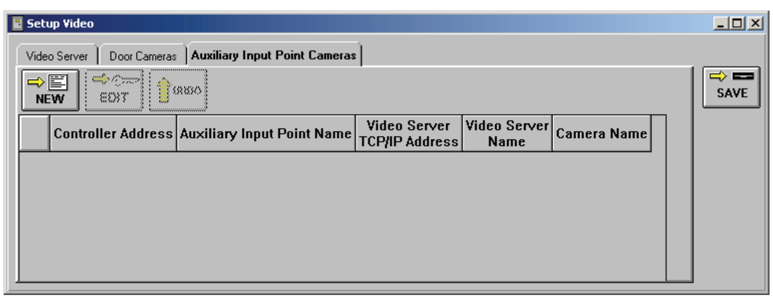


Figure 15-11: Auxiliary Input Point Cameras Window

1. Click on the  button. A new blank row appears.

Controller Address
From the pull-down list, select the controller to be assigned a camera. Only controllers with a satellite board (SB-293 or SB-593) will be available for use.

Auxiliary Input Point Name
From the pull-down list, select the input point to be assigned a camera.

Video Server TCP/IP Address
The TCP/IP address of the video server is automatically entered.

Video Server Name

The Video Server Name that was entered during the Setup Video Server process appears here.

Camera Name

From the pull-down list, select the camera to be assigned to the input point in the second column.

NOTE: More than one camera may be assigned to each input point and more than one input point may be assigned to each camera. It is all dependent on where the cameras are pointed.

2. Click on the 

button to save each row. Repeat the process for as many cameras/input point combinations there are. If the information is not saved before clicking any other button or exiting the Setup Video window, the data entered is lost and must be re-entered.
    - To make changes to a row that has already been saved, click on the row that needs changed and then click on the 

button. Make the necessary changes and click on the 

button.
    - To remove a row before it has been saved, click on the row to be removed and then click on the 

button.
    - To remove a row after it has been saved, click on the row to be removed and then click on the 

button.
3. The finished window may appear similar to Figure 15-12.

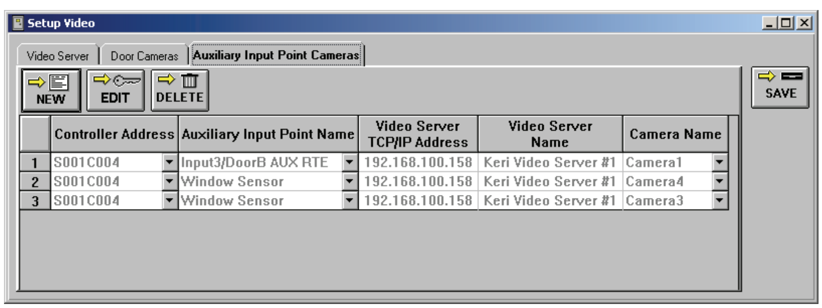


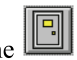
Figure 15-12: Auxiliary Input Point and Cameras Assigned


NOTE: If a camera name has been changed, DO NOT delete the Auxiliary Input Point Camera Tab setup. Add a new row for the new camera name. If the old camera setup is deleted, Doors will not be able to find any video-related events that took place prior to the camera name change.

3.0 Archiving Video Clips

Archiving of video clips must be performed separately from archiving Doors events. For more information on how to archive video clips refer to the *Visions Server Setup and Users Guide* (P/N 01975-001).

4.0 Disable Video

1. To disable Video, click on the Setup ⇒ System pull-down menu or click on the  button on the tool bar, then click on the **System Options** tab. The System Options window appears. Click on the 

button to reveal the Video field (see Figure 15-4 on page 4 of this section).
1. Click in the Video ON check box. The check mark that was there disappears and the following window appears (see Figure 15-13).

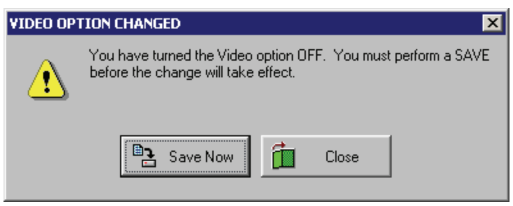


Figure 15-13: Video Option Changed - OFF

2. Click the 

button. A "Saved Configuration" window flashes on the screen.
3. Click on the 

button to save these changes. If the Video changes are not saved before clicking any other button or exiting the System Options window, the data entered is lost and must be re-entered.

End of section.

Appendix

1. Database File Field Definitions
2. Glossary

This page is intentionally left blank.

Database File Field Definitions

Certain applications may wish to import the data within a quick search event report into a spreadsheet or database program (for example, time and attendance programs). The information in this section describes the format of the data written to a quick search event report file, identifying and defining the following.

- the total number of characters that make up a single event string in a quick search event report
- the information fields within an event string
- the number of characters in each information field
- the ASCII definition of the characters in the information field
- an example string

Data Format in Single Site Mode – Using the User's Name

The following table defines the data within a quick search event report for a Doors application in Single Site mode, using the user's name to identify the user associated with an event. One event string is made up of 102 ASCII characters.

Table 1: Quick Search Event Report Data Format – Single Site Mode / User's Name

Field	Date	Delimiter	Time	Delimiter	Door	Delimiter	User	Delimiter	Event	End of Record
# of characers	10	2	8	2	32	2	23	2	19	2
Description	MM/DD/ YYYY	0x20 0x20	HH:MM:SS	0x20 0x20	Door Name padded with 0x20	0x20 0x20	User Name padded with 0x20	0x20 0x20	Event Text String padded with 0x20	0x0D 0x0A
Example	07/04/1997	<space> <space>	19:30:17	<space> <space>	Front <space> Door <5 spaces>	<space> <space>	Adams, <space> John <space> Q <10 spaces>	<space> <space>	Access <space> Granted <5 spaces>	<CR><LF>

Data Format in Single Site Mode – Using the User's Card Number

The following table defines the data within a quick search event report for a Doors application in Single Site mode, using the user's card number to identify the user associated with an event. One event string is made up of 89 ASCII characters.

Table 2: Quick Search Event Report Data Format – Single Site Mode / User's Card Number

Field	Date	Delimiter	Time	Delimiter	Door	Delimiter	Card Number	Delimiter	Event	End of Record
# of characers	10	2	8	2	32	2	10	2	19	2
Description	MM/DD/ YYYY	0x20 0x20	HH:MM:SS	0x20 0x20	Door Name padded with 0x20	0x20 0x20	User's Card Number front-padded with 0x20	0x20 0x20	Event Text String padded with 0x20	0x0D 0x0A
Example	07/04/1997	<space> <space>	19:30:17	<space> <space>	Front <space> Door <5 spaces>	<space> <space>	<4 spaces> 187491	<space> <space>	Access <space> Granted <5 spaces>	<CR><LF>

Data Format in Multiple Site Mode – Using the User's Card Number

The following table defines the data within a quick search event report for a Doors application in Multiple Site mode, using the user's card number to identify the user associated with an event. One event string is made up of 119 ASCII characters.

Table 3: Quick Search Event Report Data Format – Multiple Site Mode / User's Name

Field	Date	Delimiter	Time	Delimiter	Site	Delimiter	Door	Delimiter	Card-holder	Delimiter	Event	End of Record
# of characers	10	2	8	2	15	2	32	2	23	2	19	2
Descrip-tion	MM/DD/ YYYY	0x20 0x20	HH:MM: SS	0x20 0x20	Site Name padded with 0x20	0x20 0x20	Door Name padded with 0x20	0x20 0x20	User Name padded with 0x20	0x20 0x20	Event Text String padded with 0x20	0x0D 0x0A
Example	07/04/ 1997	<space> <space>	19:30:17	<space> <space>	Home <space> Office <4 spaces>	<space> <space>	Front <space> Door <5 spaces>	<space> <space>	Adams, <space> John <space> Q <10 spaces>	<space> <space>	Access <space> Granted <5 spaces>	<CR><LF>

Data Format in Multiple Site Mode – Using the User’s Name

The following table defines the data within a quick search event report for a Doors application in Multiple Site mode, using the user’s name to identify the user associated with an event. One event string is made up of 106 ASCII characters.

Table 4: Quick Search Event Report Data Format – Multiple Site Mode / User’s Card Number

Field	Date	Delimiter	Time	Delimiter	Site	Delimiter	Door	Delimiter	Card Number	Delimiter	Event	End of Record
# of characers	10	2	8	2	15	2	32	2	10	2	19	2
Descrip-tion	MM/DD/ YYYY	0x20 0x20	HH:MM: SS	0x20 0x20	Site Name padded with 0x20	0x20 0x20	Door Name padded with 0x20	0x20 0x20	User’s Card Number front-padded with 0x20	0x20 0x20	Event Text String padded with 0x20	0x0D 0x0A
Example	07/04/ 1997	<space> <space>	19:30:17	<space> <space>	Home <space> Office <4 spaces>	<space> <space>	Front <space> Door <5 spaces>	<space> <space>	<4 spaces> 187491	<space> <space>	Access <space> Granted <5 spaces>	<CR><LF>

This page is intentionally left blank.

Glossary

access control – Access control is a general term describing the management of the entrance and exit of people through secure areas.

access control network – An access control network is an interconnected set of controllers, managing the entrance and exit of people through secure areas.

access group – An access group combines time zones and doors into a superset of information that is applied to users. Basically an access group defines at what times and through which doors users are granted access. To be granted access to a secure door, a user must meet the criteria of the access group assigned to the user: be at a door that is a member of the access group during a time period within the time zone assigned to the access group.

address, controller – Each controller must be assigned a unique address, identifying that controller in the network. A controller address is similar to a home address. By addressing an envelope, mail is sent to a specific individual at a specific home. By assigning unique controller addresses, operating information can be sent directly to specific controllers.

alarm control – When a PXL-510 master controller is connected to a NetworX NX-8E alarm panel, any of the readers on the access control network can be set up to arm/disarm the alarm system by presenting an access card.

amnesty – Amnesty allows a card/user to violate anti passback rules and reenter a secure area that a controller has tracked as having already been entered by that card/user. (See **anti passback**.)

anti passback – Anti passback (APB) provides one-card one-way access into and out of a secure area. It prevents someone from using a card to enter a secure area and then passing that card back to someone else to use to enter that same secure area.

APB – See **anti passback**.

archive file type – The selection of the archive file type determines how event files will be archived. There are three types to choose from: yearly (default); monthly; or weekly.

aspect ratio – The aspect ratio is a scaling number based on the height versus width of a graphic. When resizing graphics, as the height changes, the width changes a corresponding amount maintaining the aspect ratio. This ensures the graphic appears correct regardless of the new size of the graphic.

auto-collection – Auto-collection allows the host computer to automatically receive event information from the controller’s event buffer, when the controller’s buffer becomes full.

auto-config – See **auto-configuration**.

auto-configuration – Auto-configuration is a process within the *Doors* software where the software polls the access control network to determine which controllers on the access control network are responding and then receive configuration information from these controllers.

banner message – The EntraGuard Gold controller may be set up to display up to three rotating banner messages on the LCD.

card – A card is an access control identification device assigned to an individual to give that individual access rights to an access control network. It is the size of a credit card. Each card has a unique identification code. That identification code is then associated with an access group to determine through which doors and at what times users are granted access.

card PIN – The Card PIN (Personal Identification Number) is a special number automatically generated and assigned to a card during enrollment when the card+PIN feature has been enabled. Only for use with a P-650 Card+PIN Proximity Reader and Keypad, PXL-250W controller, and 26-bit Wiegand access cards. This PIN allows a secondary verification of a user by requiring a PIN be entered after presenting a valid access card. The Card PIN cannot be changed or edited and must be given to the user with the card.

card number – The card number is the second set of digits printed on the body of the access control card or tag. The card number will be more than 4 digits long.

cardholder – A cardholder is an individual who has been assigned an access control card or tag.(See **user**.)

collecting events – Collecting events from all controllers clears the controller buffers and stores the events in an event file on the hard disk. Event data can then be processed into report format. Collection of events can take place while updating or while monitoring.

COM port – A COM port is a serial data communications device on a computer. Communication between the host computer and the access control network is done through this device.

connect timer – The EntraGuard connect timer determines the length of connection between the EntraGuard unit and the tenant’s telephone.

controller – A controller is a microprocessor based circuit board that manages access to a secure area. The controller receives information that it uses to determine through which doors and at what times users are granted access to that secure area. Based on that information, the controller can lock/unlock doors, sound alarms, and communicate status to a host computer.

database – A database is an organized set of information.

daylight savings adjustment – Enabling the daylight savings adjustment allows the controllers to automatically adjust the time on the controllers when daylight savings time comes and goes.

dedicated I/O point – A dedicated I/O point is an input point that is dedicated to an Auxiliary RTE function or an output point that is dedicated to single-door annunciation of Door Forced or Door Held Open alarms.

department group – A department group is an operator assigned field in the user database. It is not actively used by the *Doors* software, but is provided to allow an operator to sort the users within the database based on the department for which they work.

desktop – The desktop is the primary window in the Windows operating system, from which programs are started.

dial timezone – A dial timezone is a definition of the time-of-day and the days-of-the-week when a tenant will accept a call from visitors requesting access through the EntraGuard unit. The process to set up a Dial Timezone is the same as setting up any time zone.

dialog box – A dialog box is a text window that the *Doors* software displays on screen when the software needs information from an operator. The operator enters the information by reading the instructions in the window and then filling-in-the-blanks in designated fields in the window.

digital tablet – A digital tablet is an input device used to input a user's signature. It is made up of an electronic tablet and a stylus (a device rather like a pen or pencil). The user simply uses the stylus to write the user's name on the tablet. As the user is writing, the characters being written are displayed on screen. This digital version of the user's signature can then be used on a user's photo ID badge. (See **stylus**.)

directory code – The directory code is the set of numbers used by visitors at the EntraGuard controller to dial up the person they wish to contact. The tenant may then either grant or deny visitor access to the building.

door class – An operator may assign a class to the doors so that door commands can be performed on all doors grouped within a class.

door name – An operator can assign a descriptive name to a door on the access control system.

download – Downloading is the process by which the host computer receives information from the access control network; information is downloaded to the host computer. (See **upload**.)

dual verification –The use of two credentials to gain access into a secure area.

egress – Egress is a term for exiting a secured area. (See **ingress**.)

enroll – Enrolling is the process of activating a card for use by a user in the access control network. A card must be entered into the access control network and then assigned to a user.

EntraGuard – EntraGuard refers to the use of the EntraGuard Gold Telephone Entry controller on the access control network. This controller allows visitors to call a tenant requesting entry through an access controlled door. The tenant then has the ability to either grant or deny that request.

EntraGuard IDs –See **user ID.**

event – An event is an occurrence at a controller (such as unlocking a door, requesting to exit, forcing a door open) that generates a message stored by the controller.

firmware – Firmware is a set of operating instructions for a controller, stored on a ROM on the controller.

first person in – The First Person In (FPI) function allows an operator to determine if a door should be automatically unlocked when the unlock/lock time zone begins or if the door should not automatically unlock until after a person presenting a valid card arrives. This feature is used whenever there is a concern that employees may be delayed in arriving to a secured site (perhaps due to inclement weather).

general protection fault – A general protection fault (GPF) occurs whenever a program executes a command that the operating system considers dangerous to the operating system. When a GPF is generated, the program that generated the GPF is closed and control is returned to the operating system.

global secure – Global secure allows an operator to set a time of day at which all doors that are not under automatic control (i.e. controlled by an unlock/lock time zone) are locked.

global unlock – Global unlock is a feature that designates a specific input on the PXL-250 controller to be used to automatically unlock all doors in the access control network.

host computer – The host computer is the computer running the *Doors* software and communicating with the access control network.

ingress– Ingress is a term for entering a secured area. (See **egress**.)

input – An input is a set of points on a controller that is able to receive a signal indicating when an external device changes state. For example, the door switch input on the controller is attached to a switch on the door. Using the switch, the input is able to keep track of when the door is opened or closed; when the switch is open, the door is open and when the switch is closed, the door is closed.

log on – Log on is the process by which an operator enters a name and a password that identifies that operator to the *Doors* program. This identification is used by the program to control which commands an operator is authorized to perform and track which operations the operator does perform.

loopback plug – A loopback plug is a small, serial port connector used by the COMTEST program to verify basic operation of the host computer's COM port. It is used to route signals sent out via the COM port transmit line back to the COM port receive line. Before running the COMTEST, the loopback plug is connected to the COM port designated for use by the *Doors* software. When the test is complete, the loopback plug is removed and the communication line is connected.

menu bar – A menu bar is a horizontal field near the top of a program window of a program operating in a Windows operating system that allows a program operator to select program commands and options.

message timer – The EntraGuard message timer determines the length of time a banner message is displayed on the EntraGuard LCD before changing to the next banner message.

modem – A modem is a communication device that converts computer serial data to a format that can be transmitted and received via telephone.

monitor – A monitor is a window within the *Doors* software that tracks events that are occurring on the access control system as they happen.

multiple sites – See **site**.

off-line – The access control network is off-line when it is not actively communicating with the host computer.

online – The access control network is online when it is actively communicating with the host computer.

online help – Online help is a mini-program within the *Doors* software that provides basic descriptions and instructions for the *Doors* software. Online help can be run at the same time as the *Doors* program, side-by-side, making it easier for an operator to receive basic information regarding a program command or operation.

operator – An operator is an individual who has been granted the authority to perform certain *Doors* program managerial operations.

output – An output is a relay on a controller that is toggled, to open or close an external circuit based on either commands programmed into the controller or based on the state of an input. For example, if a door is forced open, an output relay is programmed to sound an alarm.

personal identification number – A personal identification number is a means of providing an extra level of security. PINs may be assigned to a site by an operator, allowing some operators to access a remote site, but not all; and a PIN may be assigned in connection with the P-650 Card+PIN Proximity Reader and Keypad, requiring a user to enter a personal identification number after presenting a valid access card.

PIN – An acronym for personal identification number (see **personal identification number**).

pull-down menu – When an operator clicks on an option on the menu bar, a pull-down menu appears listing all the available options for that menu selection. An operator then selects the desired operation.

radio button – Radio buttons are used whenever a program command has a set of options that require the selection of one and only one option. As an operator clicks on the radio buttons within an option set, the old selection is disabled and the new selection is enabled.

reader – A reader is a device that "reads" an identification number from a card or tag presented to the reader by a user. It then sends that identification number to the controller for processing.

report – A report is a summary of event information generated from the event log collected from all controllers on the access control network. A report may be displayed on the computer system screen, printed at a local printer, or saved to an ASCII text file for processing by another program.

request to exit – Request to Exit (RTE) is an input on the controller (or satellite board) that accepts a signal from a normally open input device. The signal indicates a request has been made by someone to exit a secured door.

ROM – A ROM is a memory device on the controller that permanently stores instructions and information. ROM stands for Read Only Memory, referring to the fact that information can only be read from the device. Information cannot be changed unless the device itself is replaced.

RTE – See **request to exit**.

shortcut – A shortcut is a command that directs a program to begin. Typically shortcuts are associated with icons placed on the Windows desktop, i.e. clicking on the *Doors* icon starts the *Doors* program.

site – A site is another term for an access control network. Site is generally used when there are more than one access control networks all being managed from one host computer. The *Doors* software within the host computer keeps track of the different access control networks by assigning each one a site number.

smart update – A smart update uploads to an access control network only the changes that have been made to an existing database.

sound alert – A sound alert is an alarm annunciation for operator selected events. Whenever a selected event occurs (if the *Doors* program is in monitor mode), an alarm sounds from the host computer that must be acknowledged by the operator by clicking on an icon on the *Doors* tool bar.

spreadsheet – A spreadsheet is an organized collection of information managed in a matrix format.

stylus – A stylus is a writing device rather like a pen or pencil. It is used in conjunction with a digital tablet to allow a user to enter a digital version of a signature for use on a photo ID badge. (See **digital tablet**.)

tag – A tag is an access control identification device assigned to an individual to give that individual access rights to an access control network. It is designed to be attached to a key-ring. Each tag has a unique identification code. That identification code is then associated with an access group to determine through which doors and at what times users are granted access.

temp users – The temp users feature allows an operator to set a future date and time for activation and expiration of a credential.

time zone – A time zone is a definition of the time-of-day and the days-of-the-week when a user may be granted access to a secure area.

tool bar – The tool bar is a set of buttons in a horizontal field beneath the menu bar, made up of shortcuts to the commonly used *Doors* program features.

unlock/lock time zone – The unlock/lock time zone is a time zone dedicated to automatically unlocking and then locking selected doors based on when the time-of-day when the time zone begins and ends. When the time zone begins, the selected doors are unlocked; when the time zone ends, the selected doors are locked.

upload – Uploading is the process by which the access control network receives information from the host computer; information is uploaded to the access control network. (See download).

user data file export/import –The user data file export/import feature allows a systems integration expert to export then import selected and limited user data to/from an external application (such as Excel ™ or some similar spreadsheet or database program).

user ID – The user ID is the code a tenant must enter on the EntraGuard controller keypad to be granted access through an EntraGuard controlled door. This number is assigned during the enrollment process.

Visions Client A PC without any special hardware running the *Visions* Client Software. The *Visions* Client connects to the *Visions* Server via LAN or modem and can view everything the Server is recording.

Visions Server A PC with a Keri System, Inc. Video Capture Card installed. The cameras are attached to it and the video clips are recorded and stored on the server hard drive.

Index

B

C

D

E

N

O

P

Q

R

S

T

U

V

W